Dr.WEB®
Enterprise Security Suite

Defend what you create

Administratorhandbuch

© Doctor Web, 2015. Alle Rechte vorbehalten

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes dard ohne Quellenangabe weder reproduziert noch auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanäle und Massenmedien verbreitet oder auf jede andere Weise benutzt werden, ausgenommen Nutzung für persönliche Zwecke.

WARENZEICHEN
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk und Dr.WEB Logo sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS
Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfälle), die sich dadurch ergeben.

Dr.Web Enterprise Security Suite
Version 10.0
Administratorhandbuch
22.07.2015

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Website: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie umfangreiche Geographie der Benutzer zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken den Benutzern für Unterstützung der Lösungen von Dr.Web-Familie!

Inhaltsverzeichnis

Kapitel 1: Dr.Web Enterprise Security Suite 8

1.1. Einleitung 8

1.2. Symbole und Abkürzungen 9

1.3. Über das Produkt 10

1.4. Systemanforderungen 16

1.5. Lieferumfang 20

1.6. Lizenzierung 21

Kapitel 2: Komponenten des Antivirus-Netzwerks und ihre Oberfläche 23

2.1. Dr.Web Server 23

2.1.1. Dr.Web Server unter Windows® verwalten 24

2.1.2. Dr.Web Server unter UNIX®-basierten Betriebssystemen verwalten 26

2.2. Dr.Web Agent 29

2.3. Dr.Web Sicherheitscenter 30

2.3.1. Administrierung 33

2.3.2. Antivirus-Netzwerk 34

2.3.3. Nachbar 40

2.3.4. Präferenzen 40

2.3.5. Hilfe 44

2.4. Komponenten des Dr.Web Sicherheitscenters 44

2.4.1. Netzwerk-Scanner 44

2.4.2. Lizenzmanager 47

2.5. Zusammenwirken von Komponenten des Antivirus-Netzwerks 55

Kapitel 3: Erste Schritte. Allgemeine Informationen 58

3.1. Einfaches Antivirus-Netzwerk erstellen 58

3.2. Netzwerkverbindungen konfigurieren 59

3.2.1. Direktverbindungen 60

3.2.2. Dr.Web Server-Suchdienst 61

3.2.3. Über SRV-Einträge 61

Kapitel 4: Administratoren des Antivirus-Netzwerks 63

4.1. Administratorauthentifizierung 63

4.1.1. Administratorauthentifizierung mithilfe der Anmeldeinformationen in der Datenbank des Servers 64

4.1.2. Authentifizierung über Active Directory 64

4.1.3. Authentifizierung mittels LDAP-Protokoll 65
4.1.4. Authentifizierung mittels RADIUS-Protokoll 66
4.1.5. Authentifizierung über PAM 67
4.2. Administratoren und administrative Gruppen 68
4.3. Administratorkonten und administrative Gruppen verwalten 70
4.3.1. Administrative Konten und Gruppen erstellen und löschen 70
4.3.2. Administrative Konten und Gruppen bearbeiten 72
Kapitel 5: Gruppen. Integrierte Verwaltung von Workstations 76
5.1. Systemgruppen und benutzerdefinierte Gruppen 76
5.2. Gruppen verwalten 79
5.2.1. Gruppen erstellen und löschen 79
5.2.2. Gruppen bearbeiten 80
5.3. Workstations zu benutzerdefinierten Gruppen hinzufügen 81
5.3.1. Workstations zu Gruppen manuell hinzufügen 82
5.3.2. Automatische Gruppenmitgliedschaft einstellen 82
5.4. Gruppenbasierte Konfiguration von Workstations 84
5.4.1. Vererbung der Workstation-Konfiguration 86
5.4.2. Einstellungen in andere Gruppen oder Workstations kopieren 87
5.5. Workstations und Gruppen vergleichen 87
Kapitel 6: Workstations verwalten 89
6.1. Workstation-Konten verwalten 89
6.1.1. Verbindungsrichtlinie für Workstations 89
6.1.2. Workstation löschen und wiederherstellen 90
6.1.3. Workstations zusammenfassen 91
6.2. Allgemeine Einstellungen der Workstation 92
6.2.1. Eigenschaften der Workstation 92
6.2.2. Installierte Komponenten des Antivirenpakets 96
6.2.3. Hardware und Software auf Workstations unter Windows® 97
6.3. Workstation konfigurieren 98
6.3.1. Berechtigungen der Workstation-Benutzer 98
6.3.2. Aufgaben für Workstations planen 100
6.3.3. Auswahl der zu installierenden Komponenten des Antivirenpakets 104
6.4. Antivirenkomponenten konfigurieren 105
6.4.1. Komponenten 106
6.4.2. Dr.Web Agent für Windows® konfigurieren 108
6.4.3. SpIDer Mail für Windows® konfigurieren. Anwendungsfilter 114

6.5. Workstations scannen 116
6.5.1. Gestartete Komponenten anzeigen und abbrechen 116
6.5.2. Gestartete Komponenten nach Typ abbrechen 116
6.5.3. Scanvorgang starten 117
6.5.4. Scanner konfigurieren 118
6.6. Statistik zu einer Workstation anzeigen 124
6.6.1. Statistik 124
6.6.2. Charts 128
6.6.3. Quarantäne 129
6.7. Installationsdateien versenden 131
6.8. Nachrichten an Workstations unter Windows® versenden 132
Kapitel 7: Dr.Web Server konfigurieren 135
7.1. Protokollierung 135
7.1.1. Dr.Web Server-Protokoll 135
7.2. Dr.Web Server konfigurieren 136
7.2.1. Allgemein 137
7.2.2. DNS 141
7.2.3. Statistik 142
7.2.4. Sicherheit 144
7.2.5. Cache 145
7.2.6. Datenbank 145
7.2.7. Proxy 146
7.2.8. Transport 147
7.2.9. Module 148
7.2.10. Cluster 148
7.2.11. Standort 149
7.2.12. Herunterladen 149
7.2.13. Gruppen-Updates 149
7.2.14. Lizenzen 151
7.3. Fernzugriff auf den Dr.Web Server 151
7.4. Zeitplan des Dr.Web Servers konfigurieren 152
7.5. Webserver konfigurieren 159
7.5.1. Allgemein 160
7.5.2. Optionen 161
7.5.3. Transport 161
7.5.4. Sicherheit 162

7.6. Benutzerprozeduren 163
7.7. Benachrichtigungen konfigurieren 164
7.7.1. Benachrichtigungskonfiguration 164
7.7.2. Benachrichtigungen der Web-Konsole 168
7.7.3. Nicht abgesendete Benachrichtigungen 169
7.8. Dr.Web Server-Repository verwalten 170
7.8.1. Status des Repository 171
7.8.2. Verschobene Aktualisierungen 171
7.8.3. Allgemeine Konfiguration des Repository 172
7.8.4. Detaillierte Konfiguration des Repository 174
7.8.5. Inhalt des Repository 177
7.9. Zusätzliche Funktionen 179
7.9.1. Datenbankverwaltung 179
7.9.2. Statistiken des Dr.Web Servers 181
7.9.3. Sicherungskopien 182
7.10. Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern 183
7.10.1. Aufbau eines Netzwerks mit mehreren Dr.Web Servern 184
7.10.2. Verbindungen zwischen Dr.Web Servern konfigurieren 186
7.10.3. Antivirus-Netzwerk mit mehreren Dr.Web Servern 190
7.10.4. Mehrere Dr.Web Server mit einer gemeinsamen Datenbank verknüpfen 192
Kapitel 8: Komponenten von Dr.Web Enterprise Security Suite aktualisieren 193
8.1. Dr.Web Server aktualisieren und aus einer Sicherungskopie wiederherstellen 193
8.2. Komponenten von Dr.Web Enterprise Security Suite manuell aktualisieren 195
8.3. Geplante Aktualisierungen 195
8.4. Repository von Dr.Web Server ohne Internetzugang aktualisieren 196
8.4.1. Repository von einem anderen Dr.Web Server kopieren 196
8.4.2. Repository über das GUS herunterladen 197
8.5. Updates für Workstations einschränken 201
8.6. Mobile Dr.Web Agents aktualisieren 202
Kapitel 9: Zusätzliche Komponenten konfigurieren 204
9.1. Proxy-Server 204
9.2. NAP Validator 207
Schlagwortregister 210

Kapitel 1: Dr.Web Enterprise Security Suite

1.1. Einleitung

Die Dokumentation für Administratoren eines auf der **Dr.Web® Enterprise Security Suite** basierten Antivirus-Netzwerks enthält sowohl allgemeine als auch detaillierte Informationen über Maßnahmen, mit denen Sie in Ihrem Unternehmen einen effizienten und umfassenden Virenschutz durch **Dr.Web® Enterprise Security Suite** implementieren können.

Die Dokumentation für den Administrator des auf der **Dr.Web® Enterprise Security Suite** basierten Antivirus-Netzwerks besteht aus folgenden Teilen:

1. **Installationsanleitung** (die Datei **drweb-esuite-10-install-manual-de.pdf**)
2. **Administratorhandbuch** (die Datei **drweb-esuite-10-admin-manual-de.pdf**)

   Dieses Administratorhandbuch richtet sich an *Administratoren des Antivirus-Netzwerks*, bzw. an die Mitarbeiter des Unternehmens, die für den Schutz der Rechner (Workstations und Server) vor Schadsoftware verantwortlich sind.

   Der Administrator des Antivirus-Netzwerks muss Systemadministratorrechte haben oder mit dem Administrator des lokalen Netzwerks zusammenarbeiten, im Bereich der Virenschutz-Strategie sachkundig sein sowie detaillierte Kenntnisse über **Dr.Web** Antivirenpakete für alle im Netzwerk verwendeten Betriebssysteme besitzen.

3. **Anhänge** (die Datei **drweb-esuite-10-appendices-de.pdf**)

Diese Administratordokumentation enthält Querverweise auf drei oben erwähnte Teile. Beim Aufrufen dieser Dokumente auf einem lokalen Rechner funktionieren diese Querverweise nur dann, wenn alle drei Dokumente unter ihren ursprünglichen Namen und im gleichen Verzeichnis abgespeichert wurden.

Die Administratordokumentation beinhaltet keine Beschreibung von **Dr.Web** Antivirenpaketen für die zu schützenden Workstations. Alle notwendigen Informationen dazu finden Sie im **Benutzerhandbuch** der jeweiligen **Dr.Web** Antivirenlösung.

Bevor Sie mit dem Lesen der Dokumente beginnen, stellen Sie sicher, dass Sie die aktuellste Ausgabe haben. Alle Handbücher werden ständig aktualisiert. Ihre aktuellsten Versionen können Sie jederzeit auf der offiziellen Website von **Doctor Web** unter http://download.drweb.com/esuite/ abrufen.

1.2. Symbole und Abkürzungen

Symbole

In diesem Administratorhandbuch werden Symbole und Hervorhebungen verwendet, die in der Tabelle 1-1 aufgeführt sind.

Tabelle 1-1: Symbole und Hervorhebungen

Symbol/Hervorhebung	Erläuterung
Beachten Sie, dass	Wichtige Bemerkung oder wichtiger Hinweis.
Achtung	Warnung vor eventuellen Fehlersituationen sowie wichtigen Momenten, die besonderer Aufmerksamkeit bedürfen.
Dr.Web Scanner	Namen von **Dr.Web** Produkten und Komponenten.
Antivirus-Netzwerk	Definition oder Link auf eine Definition.
<IP-address>	Platzhalter.
Abbrechen	Namen von Schaltflächen, Fenstern, Menüpunkten und sonstigen Bestandteilen der Benutzeroberfläche.
STRG	Bezeichnungen von Tastaturtasten.
`C:\Windows\`	Namen von Dateien und Verzeichnissen, Ausschnitte des Programmcodes.
Anhang A	Querverweis auf einen Abschnitt im Handbuch oder Hyperlink auf externe Ressourcen.

Abkürzungen

Im Handbuch werden folgende Abkürzungen bzw. Akronyme ohne nähere Erläuterung verwendet:

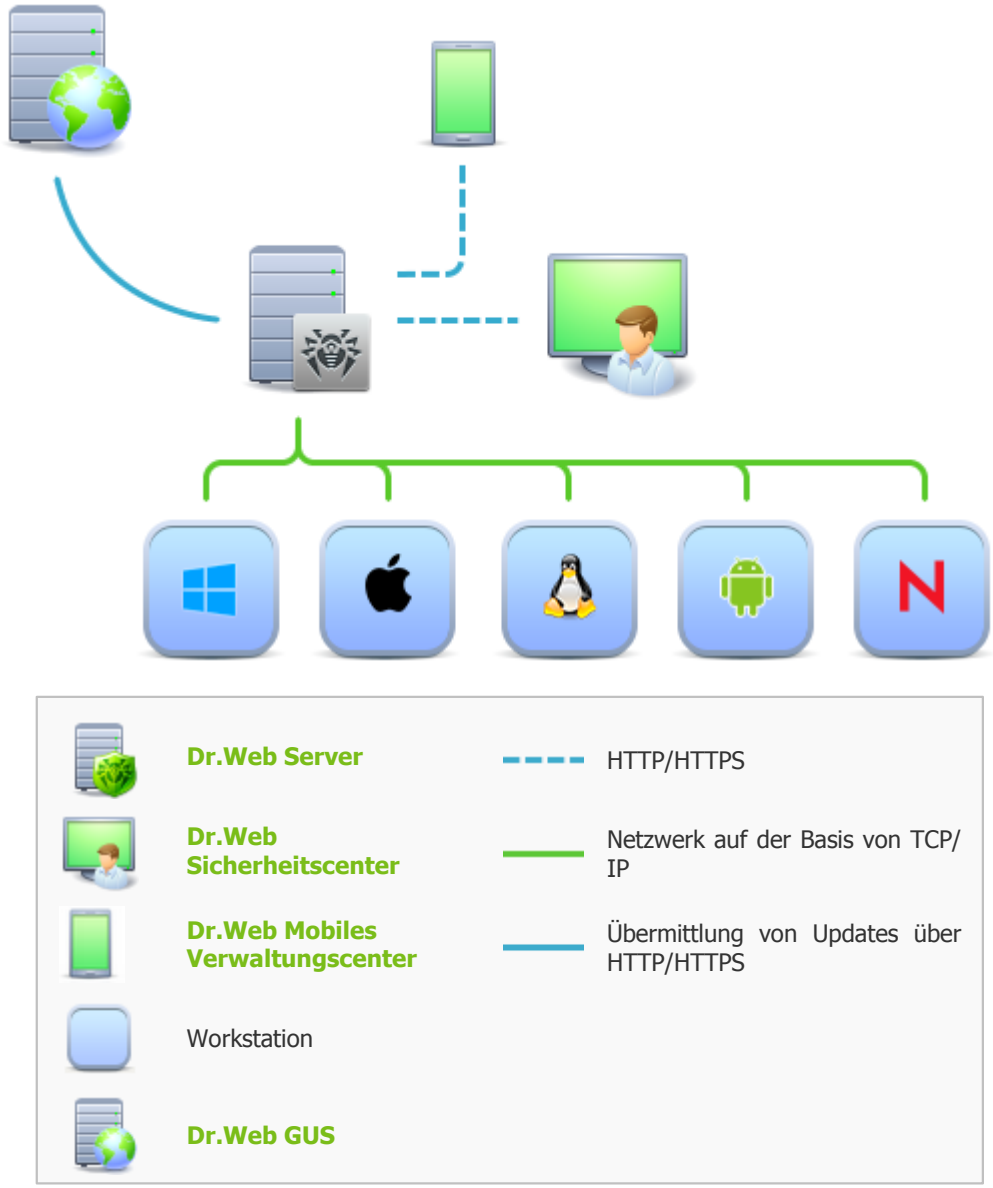
- ACL – Zugriffskontrolllisten (Access Control List)
- CDN – Netzwerk zur Auslieferung von Inhalten (Content Delivery Network)
- DFS – verteiltes Dateisystem (Distributed File System)
- DNS – System der Domänennamen (Domain Name System)
- FQDN – vollständig qualifizierter Domänenname (Fully Qualified Domain Name)
- GUI – grafische Benutzeroberfläche (Graphical User Interface), GUI-Programmversion – eine Version, die GUI-Mittel benutzt
- NAP – Network Access Protection
- MTU – maximale Paketgröße (Maximum Transmission Unit)
- TTL – Lebensdauer des Pakets (Time To Live)
- UDS – UNIX-Domain-Socket (UNIX Domain Socket)
- DB, DBMS – Datenbank, Datenbankmanagementsystem
- **Dr.Web GUS** – **Dr.Web Globales Update-System**
- LAN – lokales Netzwerk
- OS – Betriebssystem
- EBNF – erweiterte Backus-Naur-Form

1.3. Über das Produkt

Dr.Web Enterprise Security Suite bietet einen zuverlässigen zentral administrierbaren Rundumschutz interner Unternehmensnetzwerke, darunter auch mobiler Endgeräte, und privater Rechner von Mitarbeitern vor Schadsoftware jeglicher Art.

Alle Rechner und mobilen Endgeräte, auf denen die Komponenten von **Dr.Web Enterprise Security Suite** installiert sind, bilden ein einheitliches *Antivirus-Netzwerk*.

Das Antivirus-Netzwerk von **Dr.Web <%PRODCUCT%>** verfügt über eine *Client-Server-Architektur.* Seine Komponenten werden auf Rechnern und mobilen Endgeräten der Benutzer und Administratoren sowie auf LAN-Servern installiert. Die Kommunikation zwischen den Komponenten des Antivirus-Netzwerks erfolgt über TCP/IP. Die Antivirensoftware kann dabei auf den zu schützenden Workstations sowohl lokal über LAN, als auch über das Internet installiert (und später verwaltet) werden.



Logische Struktur des Antivirus-Netzwerks

Zentralschutz-Server

Der Zentralschutz-**Server** wird auf einem Rechner des Antivirus-Netzwerks installiert. Dabei kann die Installation nicht nur auf dem Rechner, der als LAN-Server verwendet wird, sondern auch auf einem beliebigen Rechner erfolgen. Die wichtigsten Anforderungen an diesen Rechner finden Sie unter Systemanforderungen.

Die plattformübergreifende Server-Software ermöglicht Ihnen, als **Server** einen Rechner unter einem der folgenden Betriebssysteme zu verwenden:

- Microsoft® Windows® Betriebssysteme
- Betriebssysteme der UNIX-Familie® (Linux®, FreeBSD®, Solaris™)

Auf dem Zentralschutz-**Server** werden Distributionen der Antivirenpakete für verschiedene Betriebssysteme, Updates von Virendatenbanken und Antivirenpaketen, Lizenzschlüssel sowie Einstellungen der Antivirenpakete der zu schützenden Workstations gespeichert. Der **Server** lädt Updates der Antivirenkomponenten von Servern des **Globalen Update-Systems** herunter und überträgt dann diese auf die zu schützenden Workstations.

Dabei können die Workstations bedienenden **Server** in einer hierarchischen Struktur miteinander verbunden werden.

Server unterstützt die Sicherung von kritischen Daten (Datenbanken, Konfigurationsdateien etc.).

Server erstellt ein einheitliches Ereignisprotokoll des Antivirus-Netzwerks.

Einheitliche Datenbank

Die einheitliche Datenbank wird mit dem Zentralschutz-**Server** verbunden. Sie enthält Statistiken zu Ereignissen im Antivirus-Netzwerk, Einstellungen des **Servers**, Parameter der Workstations und installierten Antivirenkomponenten.

Folgende Arten von Datenbanken können verwendet werden:

Eingebettete Datenbank. Zur Verfügung stehen zwei Varianten der Datenbanken, die direkt in den Zentralschutz-**Server** eingebettet sind:

- SQLite2 (InitDB)
- SQLite3

Externe Datenbank. Zur Verfügung stehen integrierte Treiber für die Verbindung der folgenden Datenbanken:

- Oracle
- PostgreSQL
- ODBC-Treiber für die Verbindung anderer Datenbanken, wie etwa Microsoft SQL Server/ Microsoft SQL Server Express

Sie können eine beliebige Datenbank verwenden, die Ihren Bedürfnissen am besten entspricht. Dazu könnte etwa das Folgende zählen: Kapazität der Datenbank, Besonderheiten der Bedienung der Datenbank-Software, Administrationsfunktionen der Datenbank, unternehmensspezifische Vorschriften und Normen.

Zentralschutz-Verwaltungscenter

Das Zentralschutz-**Verwaltungscenter** wird automatisch zusammen mit dem **Server** installiert. Es handelt sich dabei um eine Weboberfläche zur Remote-Verwaltung vom **Server** und Antivirus-Netzwerk. Dies wird durch Ändern der Einstellungen des **Servers** bzw. der Workstations, die auf dem **Server** bzw. auf den Workstations abgespeichert sind, ermöglicht.

Das **Verwaltungscenter** kann auf jedem Rechner geöffnet werden, der über einen Netzwerkzugriff auf den **Server** verfügt. Dabei kann das **Verwaltungscenter** unter fast jedem gängigen Betriebssystem in den folgenden Webbrowsern im vollen Funktionsumfang genutzt werden:

- Windows® Internet Explorer®

- Mozilla® Firefox®
- Google Chrome®

Alle Anforderungen an Webbrowser finden Sie unter Systemanforderungen.

Das Zentralschutz-**Verwaltungscenter** bietet die folgenden Möglichkeiten:

- Schnelle und leichte Installation der **Antivirensoftware** auf Workstations und Remote-Installation auf Workstations unter Windows mithilfe eines Netzwerk-Scanners; Erstellung von Distributionen mit eindeutigen IDs und Einstellungen für die Verbindung mit dem **Server**, was die Installation der **Antivirensoftware** durch Administrator erheblich erleichtert oder eventuelle Installation der **Antivirensoftware** durch Benutzer möglich macht.
- Vereinfachte Verwaltung von Workstations innerhalb des Antivirus-Netzwerks mithilfe der Gruppenverwaltung (mehr dazu finden Sie unter Kapitel 5: Gruppen. Integrierte Verwaltung von Workstations).
- Zentrale Verwaltung der Antivirenpakete von Workstations: Löschen sowohl einzelner Komponenten als auch der gesamten **Antivirensoftware** auf Workstations unter Windows; Festlegen der Parameter der Komponenten von Antivirenpaketen; Zuweisen der Rechte zur Einstellung und Verwaltung der Antivirenpakete der Workstations für Benutzer dieser Workstations (mehr dazu finden Sie unter Kapitel 6: Workstations verwalten).
- Zentrale Verwaltung von Scanvorgängen: Zeitgesteuerter Remote-Start eines Suchlaufs oder Remote-Start auf Anforderung des Administrators mithilfe des **Verwaltungscenters**; zentral verwaltetes Festlegen von an die Workstations zu übermittelnden Scan-Parametern, die zum Start eines lokalen Suchlaufs erforderlich sind (mehr dazu finden Sie im Abschnitt Workstations scannen).
- Anzeige von Statistiken zum Status der zu schützenden Workstations, zu eventuellen Bedrohungen, zum Status der installierten Antivirensoftware und gestarteten Antivirenkomponenten, sowie zur Hardware und Software von Workstations (mehr dazu finden Sie unter Statistik zu einer Workstation anzeigen).
- Flexible Verwaltung vom **Server** und Antivirus-Netzwerk durch Einschränkung der Rechte für verschiedene Administratoren; Authentifizierung von Administratoren mithilfe externer Authentifizierungssysteme, wie etwa Active Directory, LDAP, RADIUS, PAM (mehr dazu finden Sie unter Kapitel 4: Administratoren des Antivirus-Netzwerks).
- Verwaltung der Lizenzen für die auf Workstations installierte Antivirensoftware und Lizenzvergabe an Workstations, Gruppen von Workstations sowie Lizenzübertragung zwischen mehreren **Servern**, wenn das Antivirus-Netzwerk aus mehreren Servern besteht (mehr dazu finden Sie unter Lizenz-Manager).
- Umfangreiche Einstellungen zum Konfigurieren vom **Server** und seinen Komponenten, und zwar: Festlegen eines Wartungszeitplans für den **Server**; Durchführen benutzerdefinierter Prozeduren; flexibles Einstellen des Systems zum Aktualisieren aller Komponenten des Antivirus-Netzwerks über das **GUS** und anschließende Übertragung von Updates auf Workstations; Einstellen des Systems zum Benachrichtigen über Ereignisse im Antivirus-Netzwerk mit der Auswahl einer Benachrichtigungsmethode; Konfigurieren von Verbindungen zwischen den Servern, wenn das Antivirus-Netzwerk aus mehreren Servern besteht (weitere Informationen finden Sie unter Kapitel 7: Dr.Web Server konfigurieren).

Detaillierte Informationen über die Implementierung des Virenschutzes auf den Workstations finden Sie in der **Installationsanleitung**.

Ein Bestandteil des **Dr.Web Sicherheitscenters** ist der **Webserver**, der automatisch zusammen mit dem **Server** installiert wird. Der **Webserver** sorgt für die korrekte Anzeige der Seiten des **Verwaltungscenters** und stabile Client-Netzwerkverbindungen.

Mobiles Zentralschutz-Verwaltungscenter

Das **mobile Verwaltungscenter** ist eine separate Komponente, die auf mobilen Endgeräten unter iOS und Android installiert und betrieben wird. Die wichtigsten Anforderungen an diese App finden Sie unter Systemanforderungen.

Das **mobile Verwaltungscenter** wird mit dem **Server** anhand der Anmeldedaten des Administrators des Antivirus-Netzwerks, eventuell über ein verschlüsseltes Protokoll, verbunden. Das **mobile Verwaltungscenter** hat die wichtigsten Funktionen des **Verwaltungscenters**. Der Administrator des Antivirus-Netzwerks kann dadurch die zu schützenden Workstations direkt über sein mobiles Endgerät verwalten, Statistiken zu Antivirenkomponenten ansehen und Benachrichtigungen für das **mobile Verwaltungscenter** erhalten.

Sie können das **Mobile Verwaltungscenter** über das **Verwaltungscenter** oder direkt aus dem App Store oder Google Play herunterladen.

Schutz von Workstations im Netzwerk

Auf den zu schützenden Rechnern und mobilen Endgeräten des Antivirus-Netzwerks werden jeweils ein Kontrollmodul (**Agent**) und ein betriebssystemabhängiges Antivirenpaket installiert.

Die plattformübergreifende Software ermöglicht einen effektiven Virenschutz der Rechner und mobilen Endgeräte unter den folgenden Betriebssystemen:

- Microsoft® Windows® Betriebssysteme
- Betriebssysteme der UNIX-Familie®
- Mac OS® X
- Android OS
- Novell® NetWare®OS

Geschützt werden können sowohl Rechner der Benutzer als auch LAN-Server, darunter auch das E-Mail-System von Microsoft® Outlook®.

Das Kontrollmodul lädt regelmäßig vom **Server** Updates für die Antivirenkomponenten und Virendatenbanken herunter und übermittelt an den **Server** Informationen über Ereignisse auf der Workstation.

Wenn der Zentralschutz-**Server** nicht verfügbar ist, können die auf den Workstations vorhandenen Virendatenbanken direkt über das **Globale Update-System** aktualisiert werden.

Je nach Betriebssystem können die folgenden Schutzfunktionen zur Verfügung gestellt werden:

Workstations unter Microsoft® Windows®

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang (auch mit der Suche nach Rootkits) kann auch über das **Verwaltungscenter** remote ausgelöst werden.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

E-Mail-Überwachung

Scannen aller eingehenden und ausgehenden E-Mails, die durch einen E-Mail-Client übertragen werden.

Dabei kann auch ein Spam-Filter verwendet werden (sofern Ihre Lizenz diese Funktion erlaubt).

Webüberwachung

Überprüfung aller HTTP-Zugriffe auf Webseiten. Neutralisieren eventueller Bedrohungen im HTTP-Datenverkehr (z. B. in gesendeten oder empfangenen Dateien) sowie Sperren der Zugriffe auf verdächtige oder unerwünschte Ressourcen.

Office Control

Verwalten des Zugriffs auf lokale Ressourcen bzw. Netzwerkressourcen sowie Webseiten. Diese Funktion sorgt für die Integrität wichtiger Dateien, schützt sie vor dem unbeabsichtigten Ändern oder Infizieren durch Viren und verweigert Mitarbeitern den Zugriff auf unerwünschte Inhalte.

Firewall

Diese Komponente schützt Rechner vor dem unbefugten Zugriff von außen und verhindert den Verlust wichtiger Daten über das Internet. Diese Komponente überwacht Internetverbindungen und Datenübertragungen über das Internet und sperrt verdächtige Verbindungen auf der Paket- und Anwendungsebene.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Selbstschutz

Diese Komponente schützt die Dateien und Verzeichnisse von **Dr.Web Enterprise Security Suite** vor dem unbefugten oder unbeabsichtigten Löschen oder Ändern durch Benutzer bzw. bösartige Programme. Beim aktivierten Selbstschutz können nur **Dr.Web** Prozesse auf die Dateien und Verzeichnisse von **Dr.Web Enterprise Security Suite** zugreifen.

Präventivschutz

Diese Komponente sorgt für eine frühzeitige Erkennung eventueller Bedrohungen. Dabei werden Zugriffe auf kritische Objekte des Betriebssystems, Treiberladung, automatisch gestartete Programme, laufende Systemdienste und Prozesse überwacht und beim Virenfund gesperrt.

Workstations unter UNIX®

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote ausgelöst werden.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Webüberwachung

Überprüfung aller HTTP-Zugriffe auf Webseiten. Neutralisieren eventueller Bedrohungen im HTTP-Datenverkehr (z. B. in gesendeten oder empfangenen Dateien) sowie Sperren der Zugriffe auf verdächtige oder unerwünschte Ressourcen.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Workstations unter Mac OS® X

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote ausgelöst werden.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Mobile Endgeräte unter Android OS

Virenprüfung

Mobile Endgeräte werden auf Anforderung des Benutzers oder zeitgesteuert gescannt. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote gestartet werden.

Dateiüberwachung

Permanentes Echtzeit-Scannen des Dateisystems. Dabei werden auch alle Dateien gescannt, die im Speicher des mobilen Endgeräts abgespeichert werden.

Anruf- und SMS-Filter

Bei der Anruf- und SMS-Filterung werden alle unerwünschten SMS-Nachrichten und Anrufe blockiert, wie z. B. SMS-Werbung oder SMS-Nachrichten und Anrufe von unbekannten Telefonnummern und Kontakten.

Diebstahlschutz

Mit dieser Technologie können Sie Ihre verlorenen bzw. gestohlenen mobilen Endgeräte schnell lokalisieren und sperren.

Eingeschränkter Zugriff auf Internet-Ressourcen

Ein intelligenter URL-Filter schützt Nutzer der mobilen Endgeräte vor unerwünschten Internet-Ressourcen.

Firewall

Diese Komponente schützt Ihr mobiles Endgerät vor dem unbefugten Zugriff von außen und verhindert den Verlust wichtiger Daten über das Netzwerk. Diese Komponente überwacht Internetverbindungen und Datenübertragungen über das Internet und sperrt verdächtige Verbindungen auf der Paket- und Anwendungsebene.

Sicherheits-Auditor

Mit diesem Feature können Sie Ihr mobiles Endgerät auf Sicherheitslücken oder andere sicherheitsrelevante Probleme überprüfen und sie bei Bedarf rechtzeitig beheben.

Anwendungsstart-Steuerung

Diese Komponente verhindert den Start der Anwendungen, die in der Liste vertrauter Anwendungen des mobilen Endgeräts nicht eingetragen sind.

Server unter Novell® NetWare®

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Kommunikation zwischen Komponenten des Antivirus-Netzwerks

Zum Sichern einer stabilen Kommunikation zwischen Komponenten des Antivirus-Netzwerks werden die folgenden Techniken verwendet

Dr.Web Proxy-Server

Der Proxy-Server kann optional ins Antivirus-Netzwerk integriert werden. Der **Proxy-Server** dient hauptsächlich dazu, eine sichere Kommunikation zwischen dem **Server** und Workstations zu gewährleisten, wenn keine direkte Verbindung hergestellt werden kann. Das kann der Fall sein, wenn sich der **Server** und Workstations in verschiedenen Netzwerken befinden, sodass kein Paketrouting möglich ist. Durch das Zwischenspeichern kann außerdem der Netzwerkdatenverkehr verringert und die Zeit der Update-Verteilung verkürzt werden.

Datenverkehr-Kompression

Bei der Kommunikation zwischen den Komponenten des Antivirus-Netzwerks kommen besondere Komprimierungsalgorithmen zum Einsatz, die den Netzwerkdatenverkehr minimal halten.

Verschlüsselung des Datenverkehrs

Bei der Kommunikation zwischen den Komponenten des Antivirus-Netzwerks besteht es die Möglichkeit, den Datenverkehr zu verschlüsseln. Dadurch kann ein besseres Schutzniveau erzielt werden.

Zusätzliche Funktionen

NAP Validator

NAP Validator ist als optionale Komponente verfügbar und ermöglicht, die Microsoft-Technologie des Netzwerkzugriffsschutzes (NAP) zur Diagnose der auf den Workstations installierten Software zu verwenden. Dadurch können Sie sicherstellen, dass Workstations im Netzwerk den definierten Integritätsanforderungen entsprechen.

Repository Lader

Dr.Web Repository Lader ist als optionales Programm verfügbar und ermöglicht, Produkte von **Dr.Web Enterprise Security Suite** über das **Globale Update-System** herunterzuladen. Sie können dieses Tool auch dazu verwenden, um Updates für Produkte von **Dr.Web Enterprise Security Suite** herunterzuladen und sie anschließend auf einen **Server** zu übertragen, der über keine Internetverbindung verfügt.

1.4. Systemanforderungen

Damit Sie Dr.Web Enterprise Security Suite installieren und sicher betreiben können, müssen folgende Voraussetzungen erfüllt sein:

- **Dr.Web Server** muss auf einem Rechner mit Internetzugang installiert werden, um Updates über das **Dr.Web GUS** (Globale Update-System) automatisch herunterladen zu können.

Updates können an die **Server** ohne Internetverbindung übermittelt werden. Beim Antivirus-Netzwerk mit mehreren Servern können Updates nur von einem der **Server** direkt über das **GUS** heruntergeladen werden. Von diesem Server aus werden dann sie auf die anderen **Server** übertragen. Bei dem anderen Verfahren zur Update-Verbreitung wird der **Dr.Web Repository Loader** zum Herunterladen der Updates über das **GUS** verwendet. Einmal heruntergeladen, werden sie dann auf die **Server** übertragen.

- Workstations im Antivirus-Netzwerk müssen über einen Zugriff auf den **Dr.Web Server** oder **Proxy-Server** verfügen.
- Damit Antivirenkomponenten gemeinsam ordnungsgemäß funktionieren können, müssen auf den verwendeten Rechnern die folgenden Ports und Sockets geöffnet sein:

Portnummer	Protokolle	Richtung von Verbindungen	Zweck
2193	TCP	• Eingehende, ausgehende Verbindungen des **Servers** und **Proxy-Servers** • Ausgehende Verbindungen des **Dr.Web Agents**	Für Verbindung der Antivirenkomponenten mit dem **Server** und Kommunikation zwischen Servern. Die Ports werden auch vom **Proxy-Server** zur Verbindung mit Clients verwendet.
	UDP	Eingehende, ausgehende Verbindungen	Für den **Netzwerk-Scanner**.
139, 445	TCP	• Eingehende Verbindungen des **Servers** • Eingehende, ausgehende Verbindungen des **Dr.Web Agents** • Eingehende Verbindungen des Rechners, auf dem das **Verwaltungscenter** geöffnet wird	Für den **Netzwerk-Installer**.
	UDP	Eingehende, ausgehende Verbindungen	
9080	HTTP	• Eingehende Verbindungen des **Servers**	Für das **Dr.Web Sicherheitscenter**.

Portnummer	Protokolle	Richtung von Verbindungen	Zweck
9081	HTTPS	• Eingehende Verbindungen des Rechners, auf dem das **Verwaltungscenter** geöffnet wird	
10101	TCP		Für das Dienstprogramm zur Ferndiagnose des **Servers**.
80	HTTP	Ausgehende Verbindungen	Für das Herunterladen von Updates über das **GUS**.
443	HTTPS		

Beachten Sie, dass in den Versionen des **Servers 4.XX** für die Verbindung der Antivirenkomponenten mit dem **Server** der Port `2371` verwendet wurde. In der Version **10.0** wird dieser Port nicht mehr unterstützt.

Für den Dr.Web Server ist das Folgende erforderlich:

Komponente	Anforderungen
Prozessor und Betriebssystem	Folgende Betriebssysteme werden unterstützt, sofern sie auf den Rechnern mit entsprechender CPU-Leistung installiert sind: ◆ CPU mit Befehlssatzerweiterung SSE2 und 1,3 GHz Taktfrequenz oder besser: • Microsoft Windows • Linux • FreeBSD • Solaris x86-Version ◆ CPU V9 UltraSPARC IIIi oder besser: • Solaris Sparc Die vollständige Liste unterstützter Betriebssysteme finden Sie im Dokument **Anhänge**, im Anhang A.
RAM	• Mindestens: 1 GB • Empfohlen: 2 GB und mehr
Freier Speicherplatz	Mindestens 12 GB: bis 8 GB für integrierte Datenbank (Installationsverzeichnis), bis 4 GB in dem temporären Systemverzeichnis (für Arbeitsdateien). Je nach Einstellungen des **Servers** kann mehr freier Speicherplatz zum Speichern temporärer Dateien benötigt werden. Dazu zählen u. a. individuelle Installationspakete der **Agents** (jeweils ca. 8,5 MB) im Unterverzeichnis `var\installers-cache` des Installationsverzeichnisses vom **Dr.Web Server**. Bei der Installation vom **Server** muss mindestens 1,2 GB freier Speicherplatz für die Basisdistribution und 2,5 GB für die zusätzliche Distribution für den Start des Installationsprogramms und zum Entpacken der temporären Dateien auf dem Systemlaufwerk des Rechners unter Windows bzw. im Verzeichnis `/var/tmp` des Rechners unter einem Betriebssystem der UNIX-Familie (bzw. in einem anderen Verzeichnis für temporäre Dateien, wenn dieses als ihr neuer Speicherort definiert wurde) verfügbar sein. Dabei ist es nicht relevant, wo der **Server** selbst installiert wurde.
Sonstiges	Bei der Installation des **Dr.Web Servers** auf dem Rechner unter einem Betriebssystem der UNIX-Familie müssen folgende Bibliotheken vorhanden sein: `lsb 3.0` oder höher, `glibc 2.7` oder höher. Für Datenbanken des **PostgreSQL**-Datenbankmanagementsystems sind auch `libpq`-Bibliotheken erforderlich. Für Datenbanken des **Oracle**-Datenbankmanagementsystems sind auch `libaio`-Bibliotheken erforderlich.

Komponente	Anforderungen
	Darüber hinaus sind für FreeBSD die `compat-8x`-Bibliotheken erforderlich.

Für den Dr.Web Proxy-Server sind die folgenden Komponenten erforderlich:

Komponente	Anforderung
Prozessor	Intel® Pentium® III mit 667 MHz Taktfrequenz oder besser
RAM	Mindestens 1 GB
Freier Speicherplatz	Mindestens 1 GB
Betriebssystem	• Microsoft Windows • Linux • FreeBSD • Solaris Die vollständige Liste unterstützter Betriebssysteme finden Sie im Dokument **Anhänge**, im Anhang A.
Sonstiges	Bei der Installation des **Proxy-Servers** sind für Betriebssysteme der UNIX-Familie die folgenden Bibliotheken erforderlich: `lsb 3` oder höher.

Für das Dr.Web Sicherheitscenter ist das Folgende erforderlich:

- Einer der folgenden Webbrowser: Windows Internet Explorer 8 oder höher, Mozilla Firefox 25 oder höher, Google Chrome 30 oder höher

  Webbrowser Opera® 10 oder neuer, Safari® 4 oder neuer werden auch unterstützt. Dabei aber kann der volle Funktionsumfang nicht garantiert werden.

  Der volle Funktionsumfang vom **Verwaltungscenter** bei der Verwendung von Windows Internet Explorer 8 mit der aktivierten Option *Verstärkte Sicherheitskonfiguration für Internet Explorer* kann nicht garantiert werden.

  Bei der Installation des **Servers** auf einem Rechner, im wessen Namen das Zeichen „_" (Unterstrich) enthalten ist, kann der **Server** über das **Verwaltungscenter** im Windows Internet Explorer nicht gesteuert werden.

  In diesem Fall sollten Sie einen anderen Webbrowser wählen.

  Für einen korrekten Betrieb vom **Verwaltungscenter** im Windows Internet Explorer muss die IP-Adresse und/oder der DNS-Name des Rechners, auf dem der **Dr.Web Server** installiert ist, zu vertrauenswürdigen Websites des Webbrowsers hinzugefügt werden, in dem das **Verwaltungscenter** geöffnet wird.

  Damit das **Verwaltungscenter** über das Menü **Start** korrekt geöffnet wird, müssen folgende Einstellungen für den Windows Internet Explorer unter Windows 8 und Windows Server 2012 mit Kacheloberfläche festgelegt werden: **Internetoptionen** → **Programme** → **Internet Explorer wird geöffnet** – hier ist die Option **Immer mit Internet Explorer auf dem Desktop** zu aktivieren.

- Die **Browser-Erweiterung für Dr.Web Sicherheitscenter** ist für die vollwertige Nutzung des **Verwaltungscenters** erforderlich. Die Erweiterung wird zusammen mit der Distribution des **Servers** mitgeliefert und auf Anforderung des Webbrowsers bei der Arbeit mit den Elementen des **Verwaltungscenters** installiert, die das Laden der Erweiterung benötigen (für den **Netzwerk-Scanner**, bei der Remote-Installation von Antivirenkomponenten).

Um die **Browser-Erweiterung für Dr.Web Sicherheitscenter** verwenden zu können, brauchen Sie Administratorrechte (root) auf der Seite des **Netzwerk-Scanners** sowohl unter Windows als auch unter Betriebssystemen der GNU/Linux-Familie.

Bei der Verwendung des Safari-Browsers ist die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** nur für Versionen unter Windows verfügbar.

Die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** unterstützt Mozilla Firefox, Opera und Chrome für Windows oder Betriebssysteme der Linux-Familie.

- Die empfohlene Bildschirmauflösung für die optimale Anzeige des **Verwaltungscenters** beträgt 1280x1024 Pixel.

Für das Dr.Web Mobile Verwaltungscenter sind die folgenden Komponenten erforderlich:

Anforderungen unterscheiden sich je nach Betriebssystem des mobilen Geräts:

- iOS:

Komponente	Anforderung
Betriebssystem	iOS® 7 und höher
Gerät	Apple® iPhone® Apple® iPad®

- Android:

Komponente	Anforderung
Betriebssystem	Android 4.0 und höher

Für NAP ist das Folgende erforderlich:

Für Server:

- Windows Server 2008

Für Agents:

- Windows XP SP3, Windows Vista, Windows Server 2008

Für den Dr.Web Agent sowie die Vollversion des Antivirenpakets ist das Folgende erforderlich:

Die tatsächlichen Anforderungen variieren je nach Betriebssystem, auf dem die Antivirenlösung installiert wird (die vollständige Liste unterstützter Betriebssysteme finden Sie im Anhang A. Vollständige Liste unterstützter Betriebssysteme):

- Microsoft Windows:

Komponente	Anforderung
Prozessor	CPU mit 1 GHz Taktfrequenz oder besser
Freies RAM	Mindestens 512 MB
Freier Speicherplatz	Mindestens 1 GB für ausführbare Dateien, Protokolle und temporäre Dateien
Sonstiges	1. Für die korrekte Anzeige der Kontexthilfe des **Dr.Web Agents für Windows** ist der Windows® Internet Explorer® 6.0 oder neuer erforderlich. 2. Für das Plug-In **Dr.Web für Outlook** ist ein installierter Microsoft Outlook Client aus dem MS-Office-Paket erforderlich:

Komponente	Anforderung
	◆ Outlook 2000 (Outlook 9) ◆ Outlook 2002 (Outlook 10 oder Outlook XP) ◆ Office Outlook 2003 (Outlook 11) ◆ Office Outlook 2007 (Outlook 12) ◆ Office Outlook 2010 (Outlook 14) ◆ Office Outlook 2013 (Outlook 15)

- Betriebssysteme der Linux-Familie

Komponente	Anforderung
Prozessor	32-Bit-Prozessor (IA-32, x86) und 64-Bit-Prozessor (x86-64, x64, amd64) auf der Intel-Plattform
Freies RAM	Mindestens 512 MB
Freier Speicherplatz	Mindestens 400 MB freier Speicherplatz auf dem Volume, auf dem sich Verzeichnisse des **Antivirenprogramms** befinden.

- Mac OS X: Konfigurationsanforderungen entsprechen den Anforderungen für das Betriebssystem
- Android: Konfigurationsanforderungen entsprechen den Anforderungen für das Betriebssystem
- Novell Netware: Konfigurationsanforderungen entsprechen den Anforderungen für das Betriebssystem

Auf den Workstations des Antivirus-Netzwerks, das mithilfe von **Dr.Web ESS** verwaltet wird, darf keine andere Antivirensoftware installiert werden (darunter auch andere Versionen der **Dr.Web** Antivirensoftware).

Funktionen der **Agents** werden im Benutzerhandbuch für das jeweilige Betriebssystem beschrieben.

1.5. Lieferumfang

Die Distribution von Dr.Web Enterprise Security Suite wird je nach Betriebssystem des ausgewählten Dr.Web Servers geliefert:

1. Für Betriebssysteme der UNIX-Familie – als `.run`-Dateien für die Installation der folgenden Komponenten:
   - Basisdistribution des **Dr.Web Servers**
   - Zusätzliche Distribution des **Dr.Web Servers**
   - **Proxy-Server**
2. Für Microsoft Windows – als ausführbare Dateien des Installations-Assistenten der folgenden Komponenten:
   - Basisdistribution des **Dr.Web Servers**
   - Zusätzliche Distribution des **Dr.Web Servers**
   - **Proxy-Server**
   - **Dr.Web Agent** für Active Directory
   - Dienstprogramm für die Modifizierung des Active Directory-Schemas
   - Dienstprogramm für die Änderung der Attribute von Active Directory-Objekten
   - **NAP Validator**

Die Distribution des Dr.Web Servers besteht aus zwei Paketen:

1. *Basisdistribution*. Das ist die Hauptdistribution für die Installation des **Dr.Web Servers**. Ihr Inhalt entspricht dem Inhalt der Distribution der alten Versionen von **Dr.Web Enterprise Security Suite**.

   Die Basisdistribution wird auch dazu verwendet, um den **Dr.Web Server** zu installieren, der nur Antivirenpakete für Windows-Workstations enthält.

2. *Zusätzliche Distribution (extra)*. Diese beinhaltet Distributionen sämtlicher Unternehmensprodukte, die für die Installation auf Workstations unter allen unterstützten Betriebssystemen zur Verfügung gestellt werden.

   Dieser Typ der Distribution wird als Ergänzung auf den Rechnern mit bereits installierter *Basisdistribution* des **Dr.Web Servers** installiert.

Der Typ des Installationspakets der zusätzlichen Distribution muss dem der Basisdistribution entsprechen.

Die Basis-Distribution des Dr.Web Servers beinhaltet die folgenden Komponenten:

- Software des **Dr.Web Servers** für das jeweilige Betriebssystem
- Software von **Dr.Web Agents** und Antivirenpaketen für unterstützte Betriebssysteme
- Software des **Dr.Web Sicherheitscenters**
- Virendatenbanken
- Browser-Erweiterung für das **Dr.Web Sicherheitscenter**
- Browser-Erweiterung für **Dr.Web Server FrontDoor**
- Dokumentationen, Muster und Beispiele

Mit der Distribution werden auch Seriennummern mitgeliefert. Nach deren Registrierung erhalten Sie Lizenzschlüsseldateien.

1.6. Lizenzierung

Die Nutzung von **Dr.Web Enterprise Security Suite** wird anhand von Lizenzschlüsseldateien geregelt.

Jede Schlüsseldatei wird durch eine digitale Signatur vor unbefugten Änderungen geschützt. Durch eventuelle Bearbeitung wird die Datei nicht mehr gültig. Um eine zufällige Beschädigung der Datei zu vermeiden, dürfen Sie Ihre Schlüsseldatei nicht bearbeiten und/oder nach ihrem Öffnen in einem Texteditor speichern.

Der Umfang und der Preis einer Lizenz zur Nutzung der Antivirenlösung **Dr.Web Enterprise Security Suite** hängen von der Anzahl der zu schützenden Workstations innerhalb des Netzwerks ab (einschließlich Servern, die im Netzwerk von **Dr.Web Enterprise Security Suite** geschützt werden).

Teilen Sie unbedingt beim Kauf von **Dr.Web Enterprise Security Suite** dem Verkäufer der Lizenz diese Informationen mit. Der Endpreis der Lizenz hängt nicht von der Anzahl der verwendeten **Dr.Web Server** ab.

Informationen zu Besonderheiten der Lizenzierung sowie der Nutzung der Schlüsseldateien für ein bereits bestehendes Antivirus-Netzwerk finden Sie in dem Abschnitt Lizenz-Manager.

Die Lizenzschlüsseldatei kann beim Kauf zum Lieferumfang von **Dr.Web Enterprise Security Suite** gehören. In der Regel aber werden nur Seriennummern geliefert.

Die Lizenzschlüsseldatei wird an den Benutzer nach der Registrierung der Seriennummer auf der speziellen Webseite per E-Mail versendet (die Registrierung erfolgt unter http://products.drweb.com/register/, sofern keine andere Adresse auf der Registrierungskarte, die dem Produkt beigefügt wird, angegeben wurde). Besuchen Sie diese Webseite, füllen Sie das Formular mit Angaben zum Käufer aus und geben Sie ins entsprechende Feld eine Seriennummer (diese ist auf der Registrierungskarte angegeben) ein. Das Archiv mit Schlüsseldateien wird an die von Ihnen angegebene E-Mail-Adresse gesendet. Alternativ können Sie dieses Archiv direkt von der Webseite herunterladen.

Schlüsseldateien werden an den Benutzer als ZIP-Archive gesendet, die eine oder mehrere Schlüsseldateien für die zu schützenden Workstations enthalten.

Benutzer können Schlüsseldateien auf eine der folgenden Weisen erhalten:

- Per E-Mail (in der Regel nach der Registrierung auf der Webseite, siehe oben).
- Mit der Distribution des Produkts, sofern Lizenzdateien zum Distributionsumfang des Produkts gehören.
- Als Dateien auf einem separaten Datenträger.

Wir empfehlen Ihnen, Ihre Lizenzschlüsseldatei bis zum Ablauf ihrer Gültigkeitsdauer aufzubewahren und sie bei einer erneuten Installation bzw. Wiederherstellung von Programmkomponenten wieder zu verwenden. Bei Verlust der Lizenzschlüsseldatei können Sie das Registrierungsverfahren auf der oben genannten Webseite wiederholen und eine neue Lizenzschlüsseldatei erhalten. Dabei müssen Sie die gleiche Seriennummer und die gleichen Angaben zum Käufer angeben, die Sie bei der ersten Registrierung angegeben haben. Sie dürfen lediglich eine andere E-Mail-Adresse angeben. In diesem Fall wird Ihre Lizenzschlüsseldatei an die neue E-Mail-Adresse gesendet.

Um sich mit dem **Antivirenprogramm** vertraut zu machen, können Sie Demoschlüsseldateien verwenden. Solche Schlüsseldateien gewährleisten einen vollen Funktionsumfang der Hauptkomponenten, haben aber eine beschränkte Gültigkeitsdauer. Um Demoschlüsseldateien zu erhalten, füllen Sie das entsprechende Formular unter https://download.drweb.com/demoreq/biz/ aus. Ihre Anfrage wird individuell von uns geprüft. Wenn Ihre Anfrage positiv bescheidet wird, senden wir ein Archiv mit Schlüsseldateien an die von Ihnen angegebene E-Mail-Adresse.

Informationen zur Verwendung dieser Schlüsseldateien beim Installieren des Programms finden Sie im Dokument **Installationsanleitung** im Abschnitt Dr.Web Server installieren.

Kapitel 2: Komponenten des Antivirus-Netzwerks und ihre Oberfläche

2.1. Dr.Web Server

Das Antivirus-Netzwerk muss mindestens einen **Dr.Web Server** umfassen.

Zur Erhöhung der Zuverlässigkeit und Leistung des Antivirus-Netzwerks sowie zur Lastenverteilung bietet **Dr.Web Enterprise Security Suite** die Möglichkeit, ein Antivirus-Netzwerk mit mehreren **Servern** aufzubauen. In diesem Fall wird die Software gleichzeitig auf mehreren Rechnern installiert.

Dr.Web Server ist eine speicherresidente Komponente. Die Software des **Dr.Web Servers** wurde für verschiedene Betriebssysteme entwickelt (die vollständige Liste unterstützter Betriebssysteme finden Sie im Dokument **Anhänge** im Anhang A).

Grundlegende Funktionen

Dr.Web Server hat folgende Leistungsmerkmale:

- Initialisiert die Installation von Antivirenpaketen auf dem gewählten Rechner bzw. auf allen Rechner der Gruppe.
- Fragt auf jedem geschützten Rechner die Nummer der Version des Antivirenpakets, das Erstellungsdatum und die Versionsnummer der Virendatenbanken ab.
- Aktualisiert die Inhalte des Verzeichnisses der zentralen Installation sowie des Update-Verzeichnisses.
- Aktualisiert Virendatenbanken und ausführbare Dateien der Antivirenpakete sowie ausführbare Dateien der auf den Workstations installierten Komponenten des Antivirus-Netzwerks.

Informationen zum Status des Antivirus-Netzwerks sammeln

Der **Dr.Web Server** erfasst und protokolliert Daten zur Leistung der Antivirenpakete. Diese Daten werden an ihn durch die auf Workstations installierte Software (**Dr.Web** Agents, mehr dazu finden Sie unten) übermittelt. Die Informationen werden in einem gemeinsamen Ereignisprotokoll protokolliert, das eine Datenbank darstellt. In einem kleinen oder mittleren Netzwerk (bis zu 200-300 Rechnern) kann zu diesem Zweck eine eingebettete Datenbank eingesetzt werden. Bei einem großen Netzwerk besteht es die Möglichkeit, externe Datenbanken zu verwenden.

Damit eine eingebettete Datenbank eingesetzt werden kann, dürfen mit dem **Server** nicht mehr als 200-300 Workstations verbunden werden. Wenn der Rechner, auf dem **Dr.Web Server** installiert ist, über ausreichend leistungsfähige Hardware verfügt und einer geringen Auslastung durch andere Prozesse ausgesetzt ist, können dann bis zu 1000 Workstations verbunden werden.

Anderenfalls sollte eine externe Datenbank verwendet werden.

Bei der Verwendung einer externen Datenbank und bei der Verbindung mit dem **Server** von mehr als 10000 Workstations ist es empfehlenswert, mindestens die folgenden Anforderungen einzuhalten:

- Prozessor mit Taktfrequenz von 3 GHz
- Mindestens 4 GB freier Hauptspeicher für **Dr.Web Server** und mindestens 8 GB für Datenbankserver
- Ein UNIX-ähnliches Betriebssystem

Die folgenden Informationen werden erfasst und im gemeinsamen Ereignisprotokoll aufgezeichnet:

- Information zur Version der Antivirenpakete auf den Workstations
- Uhrzeit und Datum der Installation und Aktualisierung der Software der Workstation mit Angabe der Softwareversion
- Uhrzeit und Datum der Aktualisierung von Virendatenbanken mit Angabe deren Versionen
- Informationen zum Betriebssystem, das auf den Workstations installiert ist, Prozessortyp, Speicherort der Systemkataloge usw.
- Konfiguration und Betriebsmodi der Antivirenpakete (Verwendung heuristischer Methoden, Liste der zu scannenden Dateitypen, Aktionen bei Virenfund u. ä.)
- Informationen zu erkannten Bedrohungen, darunter Name des erkannten Virus, Datum der Erkennung, vorgenommene Aktionen, Ergebnis der Desinfizierung usw.

Der **Dr.Web Server** benachrichtigt den Administrator des Antivirus-Netzwerks über Ereignisse im Antivirus-Netzwerk per E-Mail oder mithilfe von standardmäßigen Windows-Broadcast-Nachrichten. Eine detaillierte Beschreibung der Einstellungen für das Benachrichtigungssystem finden Sie unter Benachrichtigungen konfigurieren.

Webserver

Der **Webserver** ist ein Bestandteil des **Dr.Web Sicherheitscenters**. Er erfüllt die folgenden Funktionen:

- Authentifizierung und Autorisierung der Administratoren am**Verwaltungscenter**
- Automatisierung des **Verwaltungscenters**
- Unterstützung der dynamisch generierten Seiten des **Verwaltungscenters**
- Unterstützung von verschlüsselten HTTPS-Verbindungen mit Clients

2.1.1. Dr.Web Server unter Windows® verwalten

Benutzeroberfläche und Verwaltung des Dr.Web Servers

Dr.Web Server verfügt über keine integrierte Oberfläche. Der **Dr.Web Server** wird in der Regel über das **Verwaltungscenter** verwaltet, das als Oberfläche des **Servers** verwendet wird.

Bei der Installation des **Servers** wird im Windows-Startmenü **Programme** das Verzeichnis **Dr.Web Server** mit den folgenden Elemente zum Konfigurieren und Verwalten des **Servers** erstellt:

- Das Verzeichnis **Serververwaltung** beinhaltet Befehle zum Starten, Neustarten und Beenden des **Servers**, Befehle zum Konfigurieren der Protokollierung sowie andere Befehle des **Servers**. Ihre detaillierte Beschreibung finden Sie im Dokument **Anhänge** unter H3. Dr.Web Server.
- Der Punkt **Weboberfläche** dient zum Aufrufen vom **Verwaltungscenter** bzw. zur Verbindung mit dem **Server**, der auf diesem Rechner installiert ist (unter http://localhost:9080).
- Der Punkt **Dokumentation** dient zum Öffnen der Administratordokumentation im HTML-Format.

Das Installationsverzeichnis des Dr.Web Servers hat die folgende Struktur:

- `bin` – beinhaltet ausführbare Dateien des **Dr.Web Servers**.
- `etc` – beinhaltet wichtige Konfigurationsdateien der Komponenten des Antivirus-Netzwerks.
- `Installer` – beinhaltet das Installationsprogramm des **Antivirenprogramms** und den öffentlichen Schlüssel (`drwcsd.pub`).
- `update-db` – beinhaltet Scripts zur Aktualisierung der Datenbank-Struktur des **Servers**.

- `var` – enthält die folgenden Unterverzeichnisse:
  - `es-dl-cache` – hier werden Installationspakete der Benutzer nach deren Erstellung zwei Wochen lang gespeichert.
  - `backup` – enthält Sicherungskopien der Datenbanken und anderer kritischer Daten.
  - `extensions` – enthält benutzerdefinierte Scripts, die bestimmte Aufgaben automatisch ausführen lassen.
  - `repository` – ist das Repository-Verzeichnis, in dem die aktuellen Updates für Virendatenbanken, Dateien der Antivirenpakete und Komponenten des Antivirus-Netzwerks abgespeichert werden. Dieses Verzeichnis enthält Unterverzeichnisse für einzelne Software-Komponenten. Diese Unterverzeichnisse enthalten ihrerseits weitere Unterverzeichnisse für die jeweiligen Betriebssysteme. Der Benutzer, unter dem der **Server** gestartet wird (in der Regel ist das der Benutzer mit dem Namen **LocalSystem**) muss über das Schreibrecht auf dieses Verzeichnis verfügen.
  - `templates` – enthält Berichtsvorlagen.
- `webmin` – enthält Elemente des **Dr.Web Sicherheitscenters**: Dokumentation, Symbole, Module.

Der Inhalt des Update-Verzeichnisses `\var\repository` wird vom Update-Server automatisch über das HTTP-Protokoll nach dem für den **Server** festgelegten Zeitplan heruntergeladen. Alternativ kann der Administrator des Antivirus-Netzwerks die neuen Updates in diese Verzeichnisse manuell kopieren.

Wichtige Konfigurationsdateien

Datei	Erläuterung	Standardverzeichnis
`agent.key` (der Name kann abweichen)	Lizenzschlüssel des **Agents**	`etc`
`certificate.pem`	SSL-Zertifikat	
`download.conf`	Netzwerkeinstellungen für die Generierung der Installationspakete des **Agents**	
`drwcsd.conf` (der Name kann abweichen)	Konfigurationsdatei des **Servers**	
`drwcsd.conf.distr`	Muster der Konfigurationsdatei des **Servers** mit Standardparametern	
`drwcsd.pri`	Privater Schlüssel	
`enterprise.key` (der Name kann abweichen)	Lizenzschlüssel des **Servers**. Die Datei wird gespeichert, falls sie nach der Aktualisierung von älteren Versionen geblieben ist. Die Datei fehlt im neuen **Server 10.0**	
`frontdoor.conf`	Konfigurationsdatei für das Dienstprogramm zur Ferndiagnose des **Servers**	
`http-alerter-certs.pem`	Zertifikate zur Verifizierung des Hosts apple-notify.drweb.com beim Versand von Push-Benachrichtigungen	
`private-key.pem`	Privater RSA-Schlüssel	
`webmin.conf`	Konfigurationsdatei des **Verwaltungscenters**	
`auth-ads.xml`	Konfigurationsdatei für die externe Active Directory-Autorisierung der Administratoren	
`auth-ldap.xml`	Konfigurationsdatei für die externe LDAP-Autorisierung der Administratoren	

Datei	Erläuterung	Standardverzeichnis
`auth-radius.xml`	Konfigurationsdatei für die externe RADIUS-Autorisierung der Administratoren	
`database.sqlite`	Eingebettete Datenbank	`var`
`drwcsd.pub`	Öffentlicher Schlüssel	• `Installer` • `webmin\install`

Dr.Web Server starten und beenden

Standardmäßig wird der **Dr.Web Server** automatisch nach der Installation sowie bei jedem Neustart des Betriebssystems gestartet.

Alternativ können Sie den **Dr.Web Server** auf eine der folgenden Weisen starten, neu starten oder beenden:

- Im Allgemeinen:
  - Über den entsprechenden Befehl, der sich unter **Start** → **Programme** → **Dr.Web Server** befindet.
  - Über die Diensteverwaltung im Bereich **Verwaltung** in der Windows-**Systemsteuerung**.
- Beenden und Neustart über das **Verwaltungscenter**:
  - Im Bereich **Administrierung**: Neustart durch Anklicken der Schaltfläche , Beenden durch Anklicken der Schaltfläche .
- Über Konsolenbefehle, die aus dem Unterverzeichnis `bin` vom Installationsverzeichnis des **Servers** ausgeführt werden müssen (mehr dazu finden Sie auch im Dokument **Anhänge** unter H3. Dr.Web Server):
  - `drwcsd start` – **Server** starten.
  - `drwcsd restart` – den **Server**-Dienst komplett neu starten.
  - `drwcsd stop` – **Server** ordnungsgemäß beenden.

Beachten Sie das Folgende: Damit der **Server** Umgebungsvariablen erkennen kann, muss er über die Diensteverwaltung oder den Konsolenbefehl neu gestartet werden.

2.1.2. Dr.Web Server unter UNIX®-basierten Betriebssystemen verwalten

Benutzeroberfläche und Verwaltung des Dr.Web Servers

Dr.Web Server verfügt über keine integrierte Oberfläche. Der **Dr.Web Server** wird in der Regel über das **Verwaltungscenter** verwaltet, das als Oberfläche des **Servers** verwendet wird.

Das Installationsverzeichnis des Dr.Web Servers hat die folgende Struktur:

`/opt/drwcs/` für Linux, Solaris und `/usr/local/drwcs` für FreeBSD:

- `bin` – beinhaltet ausführbare Dateien des **Dr.Web Servers**.
- `doc` – beinhaltet die Dateien der Lizenzvereinbarungen.
- `ds-modules`
- `fonts` – beinhaltet die Schriftarten der Benutzeroberfläche des **Verwaltungscenters**.

- `Installer` – beinhaltet den Netzwerk-Installer und den öffentlichen Schlüssel zur Installation des **Antivirenprogramms** auf zu schützenden Rechnern.
- `lib` – beinhaltet die für den **Server** erforderlichen Bibliotheken.
- `update-db` – enthält Skripte, die zur Aktualisierung der Struktur von **Server**-Datenbanken erforderlich sind.
- `webmin` – enthält alle Elemente des **Dr.Web Sicherheitscenters**.

`/var/opt/drwcs/` für Linux, Solaris und `/var/drwcs` für FreeBSD:

- `backup` – enthält Sicherungskopien der Datenbanken und anderer kritischer Daten.
- `bases` – enthält Virendatenbanken für die Abwärtskompatibilität mit früheren Versionen der **Dr.Web Agents**.
- `coredump` – enthält Absturzabbilder des **Servers**.
- `database.sqlite` – enthält die eingebettete Datenbank des **Servers**.
- `etc` – enthält Dateien mit den wichtigsten Einstellungen der Komponenten des Antivirus-Netzwerks.
- `extensions` – enthält benutzerdefinierte Scripts, die bestimmte Aufgaben automatisch ausführen lassen.
- `installers-cache` – ist der Zwischenspeicher der Installationsprogramme des **Agents**. Hier werden Installationspakete des **Agents** beim Erstellen von Workstations im **Verwaltungscenter** gespeichert.
- `log` – enthält Protokolldateien des **Servers**.
- `object` – ist der Zwischenspeicher für die Objekte des **Verwaltungscenters**.
- `reports` – ist ein temporäres Verzeichnis zum Generieren und Speichern von Protokollen.
- `repository` – ist das Update-Verzeichnis, in dem die aktuellen Updates für Virendatenbanken, Dateien der Antivirenpakete und Komponenten des Antivirus-Netzwerks abgespeichert werden. Dieses Verzeichnis enthält Unterverzeichnisse für einzelne Software-Komponenten. Diese Unterverzeichnisse enthalten ihrerseits weitere Unterverzeichnisse für die jeweiligen Betriebssysteme. Der Benutzer, unter dem der **Server** gestartet wird (in der Regel ist das der Benutzer mit dem Namen **drwcs**) muss über das Schreibrecht auf dieses Verzeichnis verfügen.
- `run` – ist die PID des **Servers**.
- `sessions` – enthält Sitzungen des **Verwaltungscenters**.
- `upload` – ist das Verzeichnis zum Herunterladen der temporären Dateien, die über das **Verwaltungscenter** konfiguriert werden (Schlüssel usw.).

`/etc/opt/drweb.com/` für Linux (nur bei der Installation mithilfe von den generischen Paketen `*.tar.gz.run`) und `/usr/local/etc/opt/` für FreeBSD:

- `software/drweb-esuite.remove` – ist das Script zum Entfernen des **Servers**.
- + eventuell zusätzliche Dateien und Verzeichnisse.

`/usr/local/etc/rc.d/` für FreeBSD:

- `drwcsd.sh` – ist das Script zum Starten und Beenden des **Servers**.

`/var/tmp/drwcs` – enthält die Sicherungskopie des entfernten **Servers**.

Wichtige Konfigurationsdateien

Datei	Erläuterung	Standardverzeichnis
`agent.key` (der Name kann abweichen)	Lizenzschlüssel des **Agents**	• Für Linux und Solaris: /var/opt/drwcs/etc
`certificate.pem`	SSL-Zertifikat	

Datei	Erläuterung	Standardverzeichnis
common.conf	Konfigurationsdatei (für einige UNIX-ähnliche Betriebssysteme)	• Für FreeBSD: /var/drwcs/etc
download.conf	Netzwerkeinstellungen für die Generierung der Installationspakete des **Agents**	
drwcsd.conf (der Name kann abweichen)	Konfigurationsdatei des **Servers**	
drwcsd.conf.distr	Muster der Konfigurationsdatei des **Servers** mit Standardparametern	
drwcsd.pri	Privater Schlüssel	
enterprise.key (der Name kann abweichen)	Lizenzschlüssel des **Servers**. Die Datei wird gespeichert, falls sie nach der Aktualisierung von älteren Versionen geblieben ist. Die Datei fehlt im neuen **Server 10.0**	
frontdoor.conf	Konfigurationsdatei für das Dienstprogramm zur Ferndiagnose des **Servers**	
http-alerter-certs.pem	Zertifikate zur Verifizierung des Hosts apple-notify.drweb.com beim Versand von Push-Benachrichtigungen.	
private-key.pem	Privater RSA-Schlüssel	
webmin.conf	Konfigurationsdatei des **Verwaltungscenters**	
auth-ldap.xml	Konfigurationsdatei für die externe LDAP-Autorisierung der Administratoren	
auth-pam.xml	Konfigurationsdatei für die externe PAM-Autorisierung der Administratoren	
auth-radius.xml	Konfigurationsdatei für die externe RADIUS-Autorisierung der Administratoren	
database.sqlite	Eingebettete Datenbank	• Für Linux und Solaris: /var/opt/drwcs • Für FreeBSD: /var/drwcs
drwcsd.pub	Öffentlicher Schlüssel	• Für Linux und Solaris: /opt/drwcs/Installer /opt/drwcs/webmin/install • Für FreeBSD: /usr/local/drwcs/Installer /usr/local/drwcs/webmin/install

Dr.Web Server starten und beenden

Standardmäßig wird der **Dr.Web Server** automatisch nach der Installation sowie bei jedem Neustart des Betriebssystems gestartet.

Alternativ können Sie den **Dr.Web Server** auf eine der folgenden Weisen starten, neu starten oder beenden:

- Beenden und Neustart über das **Verwaltungscenter**:
  - Im Bereich **Administrierung**: Neustart durch Anklicken der Schaltfläche , Beenden durch Anklicken der Schaltfläche (fehlt bei der Version unter Solaris).

- Über den entsprechenden Konsolenbefehl (mehr dazu finden Sie auch im Dokument **Anhänge** im H3. Dr.Web Server):
  - Start:
    - Für FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh start
      ```
    - Für Linux und Solaris:
      ```
      # /etc/init.d/drwcsd start
      ```
  - Neustart:
    - Für FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh restart
      ```
    - Für Linux und Solaris:
      ```
      # /etc/init.d/drwcsd restart
      ```
  - Beenden:
    - Für FreeBSD:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh stop
      ```
    - Für Linux und Solaris:
      ```
      # /etc/init.d/drwcsd stop
      ```

Beachten Sie das Folgende: Damit der **Server** Umgebungsvariablen erkennen kann, muss er über den Konsolenbefehl neu gestartet werden.

2.2. Dr.Web Agent

Eine detaillierte Beschreibung des **Agents** und seiner Funktionsweise finden Sie im Handbuch **Dr.Web® Agent für Windows. Benutzerhandbuch**.

Funktionsweise

Workstations werden vor bösartigen Programmen durch **Dr.Web** Antivirenpakete geschützt, die für verschiedene Betriebssysteme entwickelt wurden.

Im **Antivirenprogramm Dr.Web Enterprise Security Suite** werden diese Pakete durch den **Dr.Web Agent** gesteuert, der auf dem geschützten Rechner installiert wird und sich permanent im Speicher befindet. Durch die Verbindung mit dem **Dr.Web Server** kann der Administrator das **Antivirenprogramm** auf den Workstations über das **Verwaltungscenter** zentral konfigurieren, Zeitpläne für Suchläufe einrichten, Statistiken und sonstige Informationen zu Antivirenkomponenten ansehen, Scanvorgänge starten bzw. stoppen usw.

Der **Dr.Web Server** lädt Updates herunter und überträgt sie auf die mit ihm verbundenen **Agents**. Somit wird durch den **Dr.Web Agent** automatisch der optimale Virenschutz gewährleistet, sodass keine Benutzereingriffe oder speziellen EDV-Kenntnisse erforderlich sind.

Wenn aber eine Workstation vorübergehend außerhalb des Antivirus-Netzwerks ist, verwendet der **Dr.Web Agent** eine lokale Kopie der Einstellungen. Das Antivirenprogramm auf der Workstation bleibt dabei zwar voll funktionsfähig (innerhalb der Gültigkeitsdauer der Benutzerlizenz), doch werden die Virendatenbanken und Software nicht aktualisiert.

Die Aktualisierung mobiler **Agents** wird unter Mobile Dr.Web Agents aktualisieren beschrieben.

Grundlegende Funktionen

Dr.Web Agent hat folgende Leistungsmerkmale:

- Er installiert, aktualisiert und konfiguriert das **Dr.Web** Antivirenpaket, startet den Scanvorgang sowie führt sonstige Aufgaben aus, die vom **Dr.Web Server** erstellt werden.
- Er ruft die Komponenten des **Dr.Web** Antivirenpakets über eine spezielle Oberfläche auf.
- Er sendet an den **Dr.Web Server** Informationen über die Aufgabenausführung.
- Er übermittelt an den **Dr.Web Server** Benachrichtigungen über vordefinierte Ereignisse, die beim Betrieb des Antivirenpakets vorkommen.

Jeder **Dr.Web Agent** ist mit dem **Dr.Web Server** verbunden und gehört einer bzw. mehreren auf diesem **Server** registrierten Gruppen (mehr dazu finden Sie unter Systemgruppen und benutzerdefinierte Gruppen). Die Kommunikation zwischen einem **Agent** und dem erwähnten **Server** erfolgt über das Protokoll, das im lokalen Netzwerk verwendet wird (TCP/IP Version 4 oder 6).

Ein Rechner mit dem installierten **Agent** wird im Folgenden gemäß seinen Funktionen im Antivirus-Netzwerk als *Workstation* des Antivirus-Netzwerks bezeichnet. Beachten Sie, dass dieser Rechner je nach seinen Funktionen im lokalen Netzwerk sowohl als eine Workstation als auch als ein Server des lokalen Netzwerks auftreten kann.

2.3. Dr.Web Sicherheitscenter

Das **Dr.Web Sicherheitscenter** dient zur Verwaltung des Antivirus-Netzwerks (dazu zählt auch die Änderung dessen Umfangs und Struktur) bzw. seiner Komponenten sowie zur Einrichtung des **Dr.Web Servers**.

Damit das **Verwaltungscenter** im Webbrowser Windows Internet Explorer korrekt angezeigt wird, sollte die Adresse des **Verwaltungscenters** zur Liste der vertrauenswürdigen Webseiten des Webbrowsers hinzugefügt werden: **Tools** (**Extras**) → **Internet Options** (**Internetoptionen**) → **Security** (**Sicherheit**) → **Trusted Sites** (**Vertrauenswürdige Sites**).

Damit das **Verwaltungscenter** in Chrome angezeigt wird, müssen im Webbrowser Cookies aktiviert sein.

Verbindung mit dem Dr.Web Server

Auf jedem Rechner mit dem Netzwerkzugriff auf den **Dr.Web Server** ist das **Verwaltungscenter** unter der folgenden Adresse verfügbar:

`http://`<*Serveradresse*>`:9080`

oder

`https://`<*Serveradresse*>`:9081`

Geben Sie als <*Serveradresse*> die IP-Adresse oder den Domänennamen des Rechners an, auf dem der **Dr.Web Server** installiert ist.

Die Portnummern zur Verbindung über HTTP und zur sicheren Verbindung über HTTPS sind nicht identisch: `9080` bzw. `9081`.

Im Dialogfeld für die Autorisierung geben Sie den Namen und das Passwort des Administrators (standardmäßig lautet der Name des Administrators mit Vollzugriff **admin**, als Passwort soll das Passwort eingegeben werden, das Sie bei der Installation des **Servers** festgelegt haben).

Bei der Verbindung über HTTPS (verschlüsselte SSL-Verbindung) werden Sie vom Webbrowser aufgefordert, das vom **Server** verwendete Zertifikat zu bestätigen. Da das Zertifikat für Ihren Webbrowser unbekannt ist, wird möglicherweise eine Warnmeldung oder ein Sicherheitshinweis ausgegeben, dass das Zertifikat nicht vertrauenswürdig oder fehlerhaft ist. Zur Verbindung mit dem **Verwaltungscenter** muss dieses Zertifikat als gültig akzeptiert werden. Anderenfalls tritt beim Herstellen der Verbindung ein Fehler auf.

In einigen Webbrowsern, z. B. **FireFox 3** und höher, kann bei der Verbindung über HTTPS ein Fehler auftreten, sodass keine Verbindung mit dem **Verwaltungscenter** hergestellt werden kann. In diesem Fall fügen Sie das **Verwaltungscenter** zur Liste der vertrauenswürdigen Webseiten hinzu, indem Sie in der erschienenen Warnmeldung den Punkt **Ausnahme hinzufügen** wählen. Danach können Sie auf das **Verwaltungscenter** zugreifen.

Benutzeroberfläche des Dr.Web Sicherheitscenters

Das Fenster des **Verwaltungscenters** (s. Abb. 2-1) ist in eine *Hauptmenü*-Leiste und einen *Arbeitsbereich* aufgeteilt.

Arbeitsbereich

Im *Arbeitsbereich* finden sich grundlegende Funktionen des **Verwaltungscenters**. Je nach gewünschter Aktion wird der *Arbeitsbereich* in zwei bzw. drei Spalten (Fenster) aufgeteilt werden. Dabei gestaltet er sich von links nach rechts wie folgt:

- Das *Verwaltungsmenü* befindet sich immer im linken Fensterbereich.
- Je nachdem, welcher Punkt im Verwaltungsmenü gewählten wurde, wird ein oder zwei zusätzliche Fenster angezeigt. Im letzten Fall werden im rechten Fenster die Eigenschaften bzw. Einstellungen der Elemente des mittleren Fensters angezeigt.

Die Sprache der Benutzeroberfläche wird für jedes Administrator-Konto individuell eingestellt (s. den Punkt Administratorkonten verwalten).

Hauptmenü

Im Hauptmenü des **Verwaltungscenters** sind die folgenden Bereiche verfügbar:

- Administrierung
- Antivirus-Netzwerk
- Nachbar
- Suchleiste
- Name des am **Verwaltungscenter** aktuell angemeldeten Administrators
- Ereignisse
- Präferenzen
- Hilfe
- **Exit**-Schaltfläche zum Beenden der aktuellen Sitzung des **Verwaltungscenters**

Wenn die automatische Autorisierung im **Verwaltungscenter** aktiviert ist, werden beim Anklicken der **Exit**-Schaltfläche die Anmeldedaten des Administrators gelöscht.

Beim nächsten Anmelden am **Verwaltungscenter** müssen Sie sich mit Ihrem Namen und Passwort erneut autorisieren. Wenn die automatische Autorisierung aktiviert ist, werden der angegebene Name und das Passwort im Webbrowser gespeichert. Die Autorisierung beim **Verwaltungscenter** erfolgt dann automatisch (ohne Eingabe des Namens und Passworts), bis auf die **Exit**-Schaltfläche erneut geklickt wird.

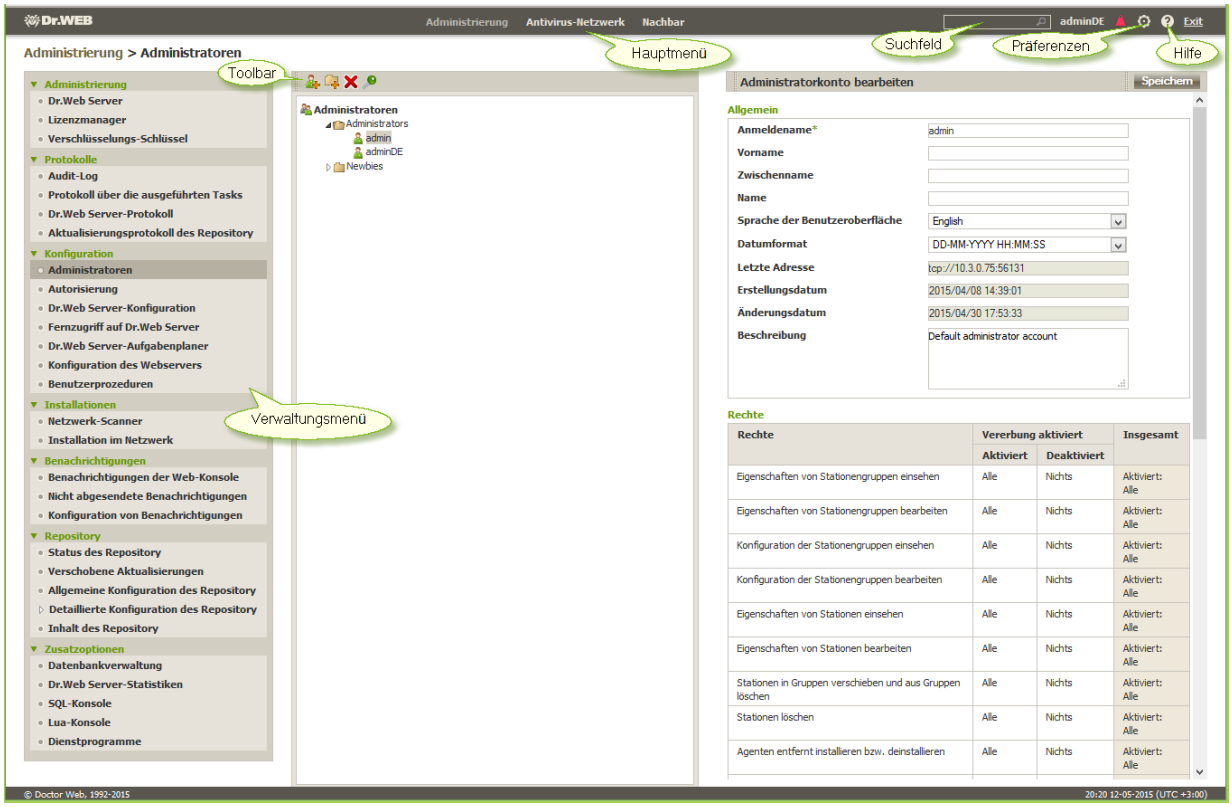


Abbildung 2-1: Das Hauptfenster des Dr.Web Sicherheitscenters. Klicken Sie auf den gewünschten Menüpunkt, um seine Beschreibung anzuzeigen

Suchleiste

Das *Suchfeld* am rechten Rand vom Hauptmenü des **Verwaltungscenters** dient zur Erleichterung der Suche nach dem gewünschten Element. Mit diesem Feld lassen sich sowohl Gruppen als auch einzelne Workstations anhand der angegebenen Parameter finden.

So finden Sie eine Workstation oder Gruppe von Workstations:

1. Wählen Sie in der Dropdown-Liste des Suchfeldes das benötigte Suchkriterium:
   - **Workstation** – um Workstations nach Namen zu suchen.
   - **Gruppe** – um Gruppen nach Namen zu suchen.
   - **ID** – um Gruppen und Workstations nach IDs zu suchen.
   - **Beschreibung** – um Gruppen und Workstations nach ihrer Beschreibung zu suchen.
   - **IP-Adresse** – um Workstations nach IP-Adressen zu suchen.
   - **Hardware** – um Workstations nach Namen der auf der Workstation installierten Hardware zu suchen.
   - **Software** – um Workstations nach Namen der auf der Workstation installierten Software zu suchen.
2. Geben Ihren Suchtext ein. Dabei können Sie festlegen, in welcher Form die eingegebene Zeichenfolge gesucht werden soll:
   - Sie können nach einer bestimmten Zeichenfolge suchen, die exakt den Suchvorgaben entspricht.

- Sie können auch Suchmasken verwenden. Als Platzhalter sind dabei die Zeichen * und ? zulässig.

3. Drücken Sie die EINGABETASTE, um die Suche zu starten.
4. In einer hierarchischen Liste werden abschließend alle Suchergebnisse angezeigt. Beachten Sie das Folgende:
   - Wenn Sie nach einer Workstation gesucht haben, wird das Vorkommen der Workstation in allen Gruppen angezeigt.
   - Wenn kein Element gefunden wurde, wird eine leere hierarchische Liste mit der Meldung **Suche ergab keine Ergebnisse** angezeigt.

2.3.1. Administrierung

Klicken Sie im Hauptmenü des **Verwaltungscenters** auf **Administrierung**. Um die Informationen im geöffneten Fenster anzusehen und zu bearbeiten, verwenden Sie das Verwaltungsmenü im linken Fensterbereich.

Das Verwaltungsmenü enthält die folgenden Punkte:

1. **Administrierung**
   - **Dr.Web Server** öffnet das Fenster, in dem Sie die wichtigsten Informationen zum **Server** einsehen und bei Bedarf ihn durch Anklicken der Schaltfläche neu starten bzw. durch Anklicken der Schaltfläche (fehlt unter Solaris) oben rechts im Fenster beenden können. Falls heruntergeladene Updates für den **Dr.Web Server** vorhanden sind, können Sie von hier aus zum Bereich Dr.Web Server-Updates wechseln, in dem verfügbare Updates und Sicherungskopien für verschiedene Versionen des **Servers** aufgeführt sind.
   - Lizenzmanager ermöglicht die Verwaltung von Lizenzschlüsseldateien.
   - **Verschlüsselungs-Schlüssel** ermöglicht den Export (die lokale Speicherung) des öffentlichen und privaten Schlüssels.
2. **Protokolle**
   - **Audit-Log** ermöglicht die Anzeige des Protokolls über die Ereignisse und Änderungen, die über das **Verwaltungscenter** vorgenommen werden.
   - **Protokoll über die ausgeführten Tasks** enthält die Liste der auf dem **Server** geplanten Aufgaben mit dem Vermerk über den Status der auszuführenden Aufgabe und eventuellen Kommentaren.
   - Dr.Web Server-Protokoll enthält die Liste der Protokolle, in denen die mit dem Betrieb des **Servers** verbundenen Ereignisse aufgezeichnet werden.
   - **Aktualisierungsprotokoll des Repository** enthält die Liste der Updates, die über das **GUS** bezogen wurden, sowie detaillierte Informationen über aktualisierte Revisionen der Produkte.
3. **Konfiguration**
   - Administratoren öffnet das Fester zur Verwaltung von Administrator-Konten des Antivirus-Netzwerks.
   - Authentifizierung öffnet das Fenster, in dem die Authentifizierung von Administratoren am **Verwaltungscenter** konfiguriert wird.
   - Dr.Web Server-Konfiguration öffnet das Fenster mit den Grundeinstellungen des **Servers**.
   - Fernzugriff auf Dr.Web Server enthält Einstellungen für die Verbindung des Dienstprogramms zur Ferndiagnose des **Servers**.
   - Dr.Web Server-Aufgabenplaner öffnet das Fenster, in dem zeitgesteuerte Aufgaben des **Servers** geplant werden.
   - Konfiguration des Webservers öffnet das Fenster mit den Grundeinstellungen des **Webservers**.
   - Benutzerprozeduren.

4. **Installationen**
   - Netzwerk-Scanner erstellt die Liste von Netzwerken, durchsucht das Netzwerk nach installierter Antivirensoftware, überprüft den Schutzstatus der Rechner und installiert bei Bedarf die Antivirensoftware.
   - **Installation im Netzwerk** erleichtert die Installation der Software des **Agents** auf bestimmten Workstations (mehr dazu finden Sie in der **Installationsanleitung** unter Dr.Web Agent über das Sicherheitscenter installieren).
5. **Benachrichtigungen**
   - Benachrichtigungen der Web-Konsole dient zur Anzeige und Verwaltung von Administrator-Benachrichtigungen, die über die Methode **Web console** empfangen wurden.
   - Nicht abgesendete Benachrichtigungen ermöglicht die Nachverfolgung und Verwaltung von Administrator-Benachrichtigungen, die anhand der Einstellungen im Bereich **Konfiguration von Benachrichtigungen** nicht gesendet werden konnten.
   - Konfiguration von Benachrichtigungen dient zur Einstellung von Administrator-Benachrichtigungen über die Ereignisse im Antivirus-Netzwerk.
6. **Repository**
   - Status des Repository bietet die Möglichkeit, den Status des Repository, darunter das Datum der letzten Aktualisierung der Repository-Komponenten und deren Status, zu überprüfen.
   - Verschobene Aktualisierungen enthält die Liste von Produkten, für die im Bereich **Detaillierte Konfiguration des Repository** das Update vorübergehend deaktiviert ist.
   - Allgemeine Konfiguration des Repository öffnet das Fenster mit den Einstellungen für die Verbindung mit dem **GUS** und Aktualisierung des Repository für alle Produkte.
   - Detaillierte Konfiguration des Repository ermöglicht eine separate Einstellung der Konfiguration von Revisionen für jedes Repository-Produkt.
   - Inhalt des Repository dient zur Anzeige und Verwaltung des aktuellen Inhalts vom Repository auf Verzeichnis- oder Dateiebene.
7. **Zusatzoptionen**
   - Datenbankverwaltung ermöglicht die Verwaltung der Datenbank, die der **Dr.Web Server** zum aktuellen Zeitpunkt verwendet.
   - Dr.Web Server-Statistiken enthält statistische Daten zum Betrieb des **Servers**.
   - **SQL-Konsole** ermöglicht Ihnen, SQL-Anfragen an die vom **Dr.Web Server** verwendete Datenbank auszuführen.
   - **Lua-Konsole** ermöglicht Ihnen, LUA-Scripts direkt in der Konsole auszuführen oder sie aus einer Datei zu importieren.
   - **Dienstprogramme** öffnet den Bereich, im dem Sie zusätzliche Dienstprogramme für **Dr.Web Enterprise Security Suite** herunterladen können:
     - Dr.Web Repository Lader dient zum Herunterladen von Produkten der **Dr.Web Enterprise Security Suite** über das **Globale Update-System**. Die grafische Version des **Dr.Web Repository Laders** ist nur unter Windows verfügbar.
     - **Das Dienstprogramm zur Ferndiagnose des Dr.Web Servers** ermöglicht Ihnen, den **Dr.Web Server** remote zu verwalten und seine Statistiken anzusehen. Die grafische Version des Dienstprogramms ist nur unter Windows verfügbar.
     - **Dr.Web Mobiles Verwaltungscenter** dient zur Administrierung eines Antivirus-Netzwerks, das auf der Basis von **Dr.Web Enterprise Security Suite** aufgebaut wurde. Dieses Tool wird auf mobilen Geräten unter iOS und Android installiert.

2.3.2. Antivirus-Netzwerk

Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**.

Verwaltungsmenü

Um die Informationen im geöffneten Fenster anzusehen und zu bearbeiten, verwenden Sie das Verwaltungsmenü im linken Fensterbereich.

Das Verwaltungsmenü enthält die folgenden Punkte:

1. **Allgemein**
   - Charts
   - Gestartete Komponenten
   - Installierte Komponenten
   - Quarantäne
   - Vergleich der Hardware und Software (wenn eine Gruppe bzw. mehrere Workstations ausgewählt sind)
   - **Nicht aktive Stationen**
   - **Benutzersitzungen**
   - Hardware und Software (wenn eine Workstation ausgewählt ist)
   - Eigenschaften
   - Gruppenregeln (wenn eine Benutzergruppe ausgewählt ist)
2. Statistik
3. **Konfiguration**
   - Rechte
   - Aufgabenplaner
   - Installierte Komponenten
   - Update-Restriktionen
   - Liste der Antivirenkomponenten für das Betriebssystem der ausgewählten Workstation bzw. je nach Betriebssystem, wenn eine Gruppe ausgewählt ist.

Die Liste der Einstellungen von Antivirenkomponenten und Empfehlungen zu ihrer Konfiguration finden Sie im **Benutzerhandbuch** für das jeweilige Betriebssystem.

Hierarchische Liste des Antivirus-Netzwerks

Im mittleren Teil des Fensters befindet sich die hierarchische Liste des Antivirus-Netzwerks. Diese Liste stellt die Baumstruktur von Elementen des Antivirus-Netzwerks dar. Die Knoten in dieser Struktur sind Gruppen und die dazugehörigen Workstations.

Sie können die folgenden Aktionen für Elemente der Liste durchführen:

- Klicken Sie mit der linken Maustaste auf den Namen der Gruppe oder Workstation, um das Verwaltungsmenü (im linken Fensterbereich) des entsprechenden Elements und Kurzangaben zur Workstation im Eigenschaftenfenster (im rechten Fensterbereich) anzeigen zu lassen.
- Klicken Sie mit der linken Maustaste auf das Symbol der Gruppe, um den Inhalt der Gruppe ein- oder auszublenden.
- Klicken Sie mit der linken Maustaste auf das Symbol der Workstation, um zum Eigenschaftenbereich dieser Workstation zu wechseln.

Um mehrere Workstations oder Gruppen in der hierarchischen Liste gleichzeitig auszuwählen, klicken Sie darauf mit der gedrückten STRG- oder UMSCHALTTASTE.

Die Darstellung des Symbols vom Element in der Liste hängt vom Typ oder Status dieses Elements ab (s. die Tabelle 2-1).

Tabelle 2-1: Symbole der Elemente in der hierarchischen Liste

Symbol	Erläuterung
	Gruppen. Allgemeine Symbole
	Gruppen, die immer in der hierarchischen Liste angezeigt werden.
	In den folgenden Fällen werden die Gruppen in der hierarchischen Liste nicht angezeigt: • Für die Gruppen wurde die Aktion **Einblenden der Gruppe einstellen** → **Ausblenden, wenn leer** angewendet, und die Gruppen enthalten zurzeit keine Workstations. • Für die Gruppen wurde die Aktion **Einblenden der Gruppe einstellen** → **Ausblenden** angewendet, und im Bereich **Einstellungen der Verzeichnisstruktur** ist das Kontrollkästchen **Ausgeblendete Gruppen anzeigen** deaktiviert.
	Workstations. Allgemeine Symbole
	Verfügbare Workstations mit installierter Antivirensoftware.
	Nicht verfügbare Workstations.
	Workstation mit deinstallierter Antivirensoftware.
	Der Status einer Workstation bei der Remote-Netzwerkinstallation des **Agents**. Die Workstation erhält diesen Status nach der erfolgreichen Installation des **Agents** und beinhaltet ihn, bis sie sich mit dem **Server** zum ersten Mal verbindet.
	Zusätzliche Symbole
	Das Symbol für individuelle Einstellungen wird auf den allgemeinen Symbolen der Gruppen und Workstations angezeigt, für die individuelle Einstellungen (bei den Gruppen auch dann, wenn die Gruppe mindestens eine Workstation mit individuellen Einstellungen hat) festgelegt sind. Um das Symbol anzeigen zu lassen, wählen Sie auf der Symbolleiste den Punkt **Einstellungen der Verzeichnisstruktur** und aktivieren Sie das Kontrollkästchen **Das Symbol für individuelle Einstellungen anzeigen**. Wenn beispielsweise für eine im Netzwerk verfügbare Workstation mit der installierten Antivirensoftware individuelle Einstellungen festgelegt sind, sieht das Symbol wie folgt aus: .
	Das Updatefehlersymbol wird neben den allgemeinen Symbolen der Workstations angezeigt, auf denen Fehler bei der Aktualisierung der Antivirensoftware auftraten. Um das Symbol anzeigen zu lassen, wählen Sie den Punkt **Einstellungen der Verzeichnisstruktur** auf der Symbolleiste und aktivieren Sie das Kontrollkästchen **Das Symbol für Update-Fehler anzeigen**. Wenn auf einer im Netzwerk verfügbaren Workstation beispielsweise ein Fehler bei der Aktualisierung der Antivirensoftware auftritt, sieht ihr Symbol wie folgt aus: .
	Das Symbol der Mitgliedschaftsregeln wird neben den allgemeinen Symbolen der Gruppen angezeigt, für die bestimmte Regeln zur automatischen Aufnahme von Workstations festgelegt sind. Um das Symbol anzeigen zu lassen, wählen Sie auf der Symbolleiste den Punkt **Einstellungen der Verzeichnisstruktur** und aktivieren Sie das Kontrollkästchen **Das Symbol für Mitgliedschaftsregeln anzeigen**. Wenn für eine Gruppe, die immer in der hierarchischen Liste angezeigt wird, bestimmte Regeln festgelegt sind, sieht ihr Symbol wie folgt aus: .

Die Elemente der hierarchischen Liste des Antivirus-Netzwerks werden über die Symbolleiste gesteuert.

Symbolleiste

Die Symbolleiste der hierarchische Liste enthält die folgenden Elemente:

Allgemein. Hier werden die allgemeinen Parameter der hierarchischen Liste gesteuert. Wählen Sie in der Dropdown-Liste den entsprechenden Punkt:

Editieren. Öffnet im rechten Teil des **Verwaltungscenters** das Fenster mit den Eigenschaften einer Gruppe oder Workstation.

Ausgewählte Objekte entfernen. Entfernt die ausgewählten Objekte der hierarchischen Liste. Sie müssen dafür in der Liste ein oder mehrere Objekte auswählen und auf **Ausgewählte Objekte entfernen** klicken.

Gruppenregeln löschen. Entfernt Regeln zur automatischen Aufnahme von Workstations in Gruppen.

Diese Gruppe als primär definieren. Durch Anklicken dieses Symbols wird eine in der hierarchischen Liste ausgewählte Gruppe als primäre Gruppe für alle dazugehörigen Workstations festgelegt.

Primärgruppe für Stationen definieren. Durch Anklicken dieses Symbols wird für die in der hierarchischen Liste ausgewählten Workstations eine primäre Gruppe festgelegt. Wenn dabei in der hierarchischen Liste eine Gruppe ausgewählt wird, wird für alle dazugehörigen Workstations die ausgewählte primäre Gruppe festgelegt.

Stationen vereinigen. Fasst Workstations in der hierarchischen Liste unter einem einheitlichen Konto zusammen. Diese Funktion wird dann verwendet, wenn eine Workstation gleichzeitig unter verschiedenen Konten registriert wurde.

Persönliche Einstellungen entfernen. Entfernt individuelle Einstellungen des in der Liste ausgewählten Objekts. In diesem Fall werden die Einstellungen der primären Gruppe verwendet. Wenn in der hierarchischen Gruppe eine Gruppe ausgewählt ist, werden die Einstellungen aller dazugehörenden Workstations entfernt.

Nachricht an Stationen senden. Durch Anklicken dieses Symbols wird an Benutzer eine Nachricht gesendet.

Passwort zurücksetzen. Setzt das benutzerdefinierte Passwort für Zugriff auf die Einstellungen der auf den Workstations installierten Antivirenkomponenten zurück. Diese Option ist verfügbar nur für Workstations unter Windows.

Station neu starten. Durch Anklicken dieses Symbols wird die gewählte Workstation remote neu gestartet.

Dr.Web Agent deinstallieren. Deinstalliert den **Agent** und die Antivirensoftware auf der gewählten Workstation bzw. Gruppe von Workstations.

Dr.Web Agent installieren. Öffnet den Netzwerk-Scanner zum Installieren des **Agents** auf den gewählten Workstations. Diese Option ist nur dann verfügbar, wenn neue genehmigte Workstations oder Workstations mit dem deinstallierten **Agent** gewählt wurden.

Gelöschte Workstations wiederherstellen. Stellt die vorher entfernten Workstations wieder her. Diese Option ist nur dann verfügbar, wenn Workstations aus der Untergruppe **Deleted** der Gruppe **Status** gewählt werden.

Installationsdateien versenden. Versendet Installationsdateien für die in der Liste gewählten Workstations an die E-Mail-Adressen, die in den Einstellungen dieses Bereichs angegeben wurden.

Station oder Gruppe hinzufügen. Erstellt ein neues Element des Antivirus-Netzwerks. Wählen Sie in der Dropdown-Liste den entsprechenden Punkt:

Station erstellen. Erstellt eine neue Workstation (mehr dazu finden Sie in der **Installationsanleitung** unter Neues Konto erstellen).

Gruppe erstellen. Erstellt eine Gruppe von Workstations.

Daten exportieren. Exportiert Daten über die Workstations des Antivirus-Netzwerks in eine CSV-, HTML- oder XML-Datei. In der Dropdown-Liste stehen für den Export die folgenden Formate zur Verfügung:

- **Im CSV-Format speichern**.
- **Im HTML-Format speichern**.
- **Im XML-Format speichern**.
- **Im PDF-Format speichern**.
- **Konfiguration exportieren**.
- **Konfiguration importieren**.
- **Konfiguration weitergeben**.

Einblenden der Gruppe einstellen. Ändert die Sichtbarkeit von Gruppen. Um die Sichtbarkeit der in der Liste gewählten Gruppe zu ändern, wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus (dabei ändert sich das Symbol der Gruppe, s. die Tabelle 2-1):

- **Ausblenden** – die Gruppe wird in der hierarchischen Liste nicht angezeigt.
- **Ausblenden, wenn leer** – die Gruppe wird in der hierarchischen Liste nicht angezeigt, wenn diese Gruppe leer ist (keine Workstations enthält).
- **Einblenden** – die Gruppe wird in der hierarchischen Liste immer angezeigt.

Komponentenverwaltung. Diese Option ermöglicht die Verwaltung der auf Workstations installierten Antivirenkomponenten. Wählen Sie dafür in der Dropdown-Liste eine der folgenden Optionen:

Fehlkomponenten aktualisieren. Erzwingt die Synchronisierung der Komponenten, die nicht aktualisiert werden konnten.

Alle Komponenten aktualisieren. Erzwingt die Aktualisierung aller installierten Komponenten in den Situationen, wenn der **Agent** beispielsweise lange Zeit keine Verbindung mit dem **Server** herstellt usw. (mehr dazu finden Sie unter Komponenten von Dr.Web Enterprise Security Suite manuell aktualisieren).

Gestartete Komponenten abbrechen. Erzwingt das Anhalten der auf der Workstation gestarteten Antivirenkomponenten.

Scannen. Startet auf der Workstation einen Scanvorgang in einem der folgenden Scanmodi:

Dr.Web Scanner. Schnell. In diesem Modus werden durch den **Dr.Web Agent Scanner** die folgenden Objekte gescannt:

- Arbeitsspeicher
- Startsektoren aller Festplatten
- Autostart-Objekte
- Stammverzeichnis des Startsektors
- Stammverzeichnis des Windows-Laufwerks
- Windows-Systemverzeichnis
- Ordner `Eigene Dateien`
- TEMP-Verzeichnis des Systems
- TEMP-Verzeichnis des Benutzers

Dr.Web Scanner. Vollständig. In diesem Modus werden alle Festplatten und Wechseldatenträger (darunter auch Startsektoren) durch den **Dr.Web Agent Scanner** komplett gescannt.

Dr.Web Scanner. Benutzerdefiniert. Dieser Modus bietet Ihnen die Möglichkeit, die gewünschten Verzeichnisse und Dateien durch den **Dr.Web Agent Scanner** scannen zu lassen.

Nicht bestätigte Stationen. Ermöglicht die Verwaltung der Liste von Anfängern. Bei einem Anfänger handelt es sich um eine Workstation, deren Registrierung noch nicht bestätigt ist. Dieser Punkt ist verfügbar nur bei der Auswahl einer Workstation aus der Untergruppe **Newbies** der Gruppe **Status**. Wird die Registrierung bestätigt bzw. der Zugriff auf den **Server** verweigert, werden die Workstations aus der vordefinierten Untergruppe **Newbies** automatisch gelöscht. Wählen Sie dafür in der Dropdown-Liste eine der folgenden Optionen aus:

Zugriff für die ausgewählten Stationen erlauben und Gruppe als primär definieren. Erzwingt die Bestätigung des Zugriffs der Workstation auf den **Server** und die Festlegung einer Primärgruppe aus der angebotenen Liste.

Die zur Ausführung definierte Aktion beim Verbindungsaufbau zurücksetzen. Erzwingt den Abbruch der Aktion für eine nicht bestätigte Workstation, deren Durchführung bei der Verbindung der Workstation mit dem **Server** geplant wurde.

Ausgewählten Stationen Zugriff verbieten. Verweigert der Workstation den Zugriff auf den **Server**.

Einstellungen der Verzeichnisstruktur. Hier wird die Strukturansicht der Liste angepasst.

- Für Gruppen:
  - **Mitgliedschaft in allen Gruppen** – gibt an, dass eine Workstation in allen Gruppen angezeigt wird, in die sie aufgenommen wurde (gilt nur für Gruppen, die mit dem weißen Ordnersymbol markiert sind. Siehe die Tabelle 2-1). Wenn das Kontrollkästchen aktiviert ist, wird die Workstation in allen Mitgliedergruppen angezeigt. Beim deaktivierten Kontrollkästchen wird die Workstation nur im oberen weißen Ordner angezeigt.
  - **Ausgeblendete Gruppen anzeigen** – erzwingt die Anzeige aller Gruppen, die zum Antivirus-Netzwerk gehören. Wenn das Kontrollkästchen deaktiviert ist, werden alle leeren Gruppen (ohne Workstations) ausgeblendet. Dies kann sinnvoll sein, wenn überflüssige Informationen ausgeblendet werden müssen, z. B. falls zu viele leere Gruppen vorhanden sind.
- Für Workstations:
  - **Stations-ID anzeigen** – aktiviert bzw. deaktiviert die Anzeige der IDs von Workstations in der hierarchischen Liste.
  - **Stationsnamen anzeigen** – aktiviert bzw. deaktiviert die Anzeige der Namen von Workstations.
  - **Stationsadressen anzeigen** – aktiviert bzw. deaktiviert die Anzeige der IP-Adressen von Workstations in der hierarchischen Liste.
  - **Stationsserver anzeigen** – aktiviert bzw. deaktiviert die Anzeige der Namen oder IP-Adressen der Antivirus-**Server**, mit denen Workstations verbunden sind.
  - **Das Symbol für Update-Fehler anzeigen** – aktiviert bzw. deaktiviert die Anzeige des Updatefehlersymbols auf den Symbolen der Workstations, die nicht aktualisiert werden konnten.
- Für alle Elemente:
  - **Das Symbol für individuelle Einstellungen anzeigen** – gibt an, ob das entsprechende Symbol auf den Symbolen der Workstations und Gruppen angezeigt werden soll, für welche individuelle Einstellungen festgelegt sind.
  - **Beschreibungen anzeigen** – gibt an, ob die optionale Beschreibung für Workstations und Gruppen angezeigt werden soll. Eine Beschreibung kann in den Eigenschaften des Elements hinzugefügt werden.
  - **Anzahl von Workstations anzeigen** – gibt an, ob für alle Gruppen im Antivirus-Netzwerk die Anzahl von Workstations angezeigt werden soll.
  - **Das Symbol für Mitgliedschaftsregeln anzeigen** – aktiviert bzw. deaktiviert die Anzeige des Symbols auf den Symbolen der Workstations, die zur Gruppe anhand der Mitgliedschaftsregeln automatisch hinzugefügt wurden, und auf den Symbolen der Gruppen, zu denen die Workstations automatisch hinzugefügt wurden.

Eigenschaftenfenster

Das Eigenschaftenfenster dient zur Anzeige der Eigenschaften und Einstellungen von Workstations und Gruppen.

So bekommen Sie das Eigenschaftenfenster angezeigt

1. Klicken in der hierarchischen Liste auf den Namen der Workstation oder Gruppe und wählen Sie auf der Symbolleiste **Allgemein** → **Editieren**.
2. Im rechten Fensterbereich des **Verwaltungscenters** öffnet sich das Fenster mit den Eigenschaften der gewählten Gruppe oder Workstation. Alle hier verfügbaren Einstellungen werden unter Gruppen bearbeiten und Eigenschaften der Workstation detailliert beschrieben.

2.3.3. Nachbar

Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Nachbar**. Um die gewünschten Informationen anzusehen, verwenden Sie das Verwaltungsmenü im linken Fensterbereich.

Administrierung

Der Bereich **Administrierung** des Verwaltungsmenüs enthält den Punkt **Nachbar**, der zur Steuerung der Kommunikation zwischen **Servern** in einem Antivirus-Netzwerk mit mehreren Servern dient (mehr dazu finden Sie unter Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern).

In der hierarchischen Liste werden alle **Dr.Web Server** aufgeführt, die mit diesem **Server** verbunden sind.

Die Vorgehensweise beim Erstellen neuer Verbindungen zwischen den Servern wird im Abschnitt Verbindungen zwischen Dr.Web Servern konfigurieren beschrieben.

Tabellen

Der Bereich **Tabellen** des Verwaltungsmenüs enthält Informationen zum Betrieb des Antivirus-Netzwerks, die von anderen **Servern** empfangen werden (mehr dazu finden Sie unter Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern).

Um Zusammenfassungstabellen mit den Daten zu anderen **Servern** anzusehen, klicken Sie im Bereich **Tabellen** auf den entsprechenden Punkt.

2.3.4. Präferenzen

Um zu den Einstellungen des **Verwaltungscenters** zu wechseln, klicken Sie im Hauptmenü auf .

Alle Einstellungen in diesem Bereich gelten nur für das aktuelle Administratorkonto.

Das Verwaltungsmenü im linken Fensterbereich enthält die folgenden Elemente:

- **Mein Konto**
- **Benutzeroberfläche**
- **Abonnement**

Mein Konto

In diesem Bereich wird das aktuelle Administrator-Konto des Antivirus-Netzwerks verwaltet (s. auch den Punkt Administratoren und administrative Gruppen).

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

Sie können bei Bedarf die folgenden Einstellungen bearbeiten:

- **Anmeldename** des Administrators. Anmeldename für den Zugriff auf das **Verwaltungscenter**.
- Vollständiger Name des Administrators.
- **Sprache der Benutzeroberfläche**, die vom aktuellen Administrator verwendet wird.
- **Datumsformat**, das vom aktuellen Administrator beim Bearbeiten von den Einstellungen, die ein Datum enthalten, verwendet wird. Zur Verfügung stehen die folgenden Formate:
  - `DD-MM-YYYY HH:MM:SS`
  - `MM/DD/YYYY HH:MM:SS`
- **Beschreibung** des Kontos.
- Um das Passwort zu ändern, klicken Sie in der Symbolleiste auf **Passwort ändern**.

Die folgenden Einstellungen sind schreibgeschützt:

- Erstellungsdatum des Kontos sowie das Datum der letzten Änderung seiner Einstellungen.
- **Letzte Adresse**. Hier wird die Netzwerkadresse der letzten Verbindung unter diesem Konto angezeigt.

Administratorrechte

Die Beschreibung der Administratorrechte sowie Informationen zu deren Bearbeitung finden Sie im Abschnitt Administratoren bearbeiten.

Klicken Sie zur Bestätigung der Änderungen auf **Speichern**.

Benutzeroberfläche

Einstellungen der Verzeichnisstruktur

Die Einstellungen in diesem Unterbereich dienen zur Änderung der Strukturansicht der Liste und sind den Einstellungen ähnlich, die sich im Hauptmenü-Bereich **Antivirus-Netzwerk** auf der Symbolleiste unter der Option befinden:

- Für Gruppen:
  - **Mitgliedschaft in allen Gruppen** – gibt an, dass eine Workstation in allen Gruppen angezeigt wird, in die sie aufgenommen wurde (gilt nur für Gruppen, die mit dem weißen Ordnersymbol markiert sind. Siehe die Tabelle 2-1). Wenn das Kontrollkästchen aktiviert ist, wird die Workstation in allen Mitgliedergruppen angezeigt. Beim deaktivierten Kontrollkästchen wird die Workstation nur im oberen weißen Ordner angezeigt.
  - **Ausgeblendete Gruppen anzeigen** – erzwingt die Anzeige aller Gruppen, die zum Antivirus-Netzwerk gehören. Wenn das Kontrollkästchen deaktiviert ist, werden alle leeren Gruppen (ohne Workstations) ausgeblendet. Dies kann sinnvoll sein, wenn überflüssige Informationen ausgeblendet werden müssen, z. B. falls zu viele leere Gruppen vorhanden sind.
- Für Workstations:
  - **Stations-ID anzeigen** – aktiviert bzw. deaktiviert die Anzeige der IDs von Workstations in der hierarchischen Liste.

- **Stationsnamen anzeigen** – aktiviert bzw. deaktiviert die Anzeige der Namen von Workstations.
- **Stationsadressen anzeigen** – aktiviert bzw. deaktiviert die Anzeige der IP-Adressen von Workstations in der hierarchischen Liste.
- **Stationsserver anzeigen** – aktiviert bzw. deaktiviert die Anzeige der Namen oder IP-Adressen der Antivirus-**Server**, mit denen Workstations verbunden sind.
- **Das Symbol für Update-Fehler anzeigen** – aktiviert bzw. deaktiviert die Anzeige des Updatefehlersymbols auf den Symbolen der Workstations, die nicht aktualisiert werden konnten.

◆ Für alle Elemente:

- **Das Symbol für individuelle Einstellungen anzeigen** – gibt an, ob das entsprechende Symbol auf den Symbolen der Workstations und Gruppen angezeigt werden soll, für welche individuelle Einstellungen festgelegt sind.
- **Beschreibungen anzeigen** – gibt an, ob die optionale Beschreibung für Workstations und Gruppen angezeigt werden soll. Eine Beschreibung kann in den Eigenschaften des Elements hinzugefügt werden.
- **Anzahl von Workstations anzeigen** – gibt an, ob für alle Gruppen im Antivirus-Netzwerk die Anzahl von Workstations angezeigt werden soll.
- **Das Symbol für Mitgliedschaftsregeln anzeigen** – aktiviert bzw. deaktiviert die Anzeige des Symbols auf den Symbolen der Workstations, die zur Gruppe anhand der Mitgliedschaftsregeln automatisch hinzugefügt wurden, und auf den Symbolen der Gruppen, zu denen die Workstations automatisch hinzugefügt wurden.

Netzwerk-Scanner

Um den **Netzwerk-Scanner** verwenden zu können, müssen Sie die Browser-Erweiterung für das **Dr.Web Sicherheitscenter** installieren.

In diesem Unterbereich können Sie die Standard-Einstellungen des Netzwerk-Scanners festlegen.

Um den **Netzwerk-Scanner** zu starten, wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im Verwaltungsmenü den Punkt **Netzwerk-Scanner**.

Legen Sie die folgenden Einstellungen des **Netzwerk-Scanners** fest:

1. Legen Sie im Eingabefeld **Netzwerke** die Liste der Netzwerke im folgenden Format fest:
   - ◆ Durch einen Bindestrich getrennt (z.B. `10.4.0.1-10.4.0.10`).
   - ◆ Durch ein Komma und Leerzeichen getrennt (z. B. `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`).
   - ◆ Durch Angabe eines Netzwerkpräfixes (z.B. `10.4.0.0/24`).
2. Ändern Sie bei Bedarf den **Port** und den Wert des Parameters **Timeout (Sek.)**.
3. Um die Standardwerte zu speichern, klicken Sie auf **Speichern**. Diese Parameter werden dann bei der Verwendung des Netzwerk-Scanners automatisch festgelegt.

Zeitintervall

In diesem Unterbereich werden die Einstellungen des Zeitintervalls festgelegt, innerhalb dessen die statistischen Daten angezeigt werden sollen (mehr dazu finden Sie unter Statistik zu einer Workstation anzeigen):

◆ In der Dropdown-Liste **Standard-Zeitintervall für das Einsehen der Statistik** wird ein Zeitintervall festgelegt, das als Standard-Zeitintervall für alle Statistikbereiche verwendet wird.

Beim ersten Öffnen der Seite wird die Statistik für den festgelegten Zeitraum angezeigt. Sie können bei Bedarf das Zeitintervall direkt in den jeweiligen Statistikbereichen ändern.

◆ Damit das zuletzt festgelegte Zeitintervall für Statistikbereiche gespeichert wird, aktivieren Sie das Kontrollkästchen **Letztes Zeitintervall für das Einsehen der Statistik speichern**.

Bei der aktivierten Option wird beim ersten Öffnen der Seite die Statistik für den im Webbrowser ausgewählten Zeitraum angezeigt.

Bei der deaktivierten Option wird beim ersten Öffnen der Seite die Statistik für den im Bereich **Standard-Zeitintervall für das Einsehen der Statistik** festgelegten Zeitraum angezeigt.

Autorisierung

Aktivieren Sie das Kontrollkästchen **Automatische Autorisierung**, um die automatische Autorisierung im aktuellen Webbrowser für alle **Dr.Web Verwaltungscenter** mit einem gleichen Benutzernamen und Passwort des Administrators zuzulassen.

Nachdem das Kontrollkästchen aktiviert wurde, werden der Name und das Passwort, die vom Administrator bei der nächsten Anmeldung am **Dr.Web Sicherheitscenter** angegeben werden, über die **Browser-Erweiterung für Dr.Web Sicherheitscenter** gespeichert.

Um die automatische Autorisierung verwenden zu können, müssen Sie die Browser-Erweiterung für das **Dr.Web Sicherheitscenter** installieren.

Beim nächsten Öffnen eines beliebigen **Dr.Web Sicherheitscenters** wird die Autorisierung in diesem Webbrowser automatisch ausgeführt, vorausgesetzt dass auf dem **Server** ein Benutzer mit diesem Namen und Passwort vorhanden ist. Wenn der Name und das Passwort nicht übereinstimmen (z.B. der Benutzer fehlt bzw. der Benutzer mit diesem Namen hat ein anderes Passwort), wird das Standard-Autorisierungsfenster des **Verwaltungscenters** angezeigt.

Beim Anklicken der Schaltfläche **Exit** werden im Hauptmenü der Benutzeroberfläche des **Verwaltungscenters** die Informationen über den Namen und das Passwort des Administrators gelöscht.

Beim nächsten Anmelden am **Verwaltungscenter** müssen Sie sich mit Ihrem Namen und Passwort erneut autorisieren. Wenn die automatische Autorisierung aktiviert ist, werden der angegebene Name und das Passwort im Webbrowser gespeichert. Die Autorisierung beim **Verwaltungscenter** erfolgt dann automatisch (ohne Eingabe des Namens und Passworts), bis auf die **Exit**-Schaltfläche erneut geklickt wird.

Wählen Sie in der Dropdown-Liste **Sitzungsdauer** einen Zeitraum, nach dessen Ablauf die Sitzung des **Verwaltungscenters** im Webbrowser automatisch abgebrochen wird.

Als PDF exportieren

In diesem Unterbereich werden die Texteinstellungen beim PDF-Export von statistischen Daten festgelegt:

- In der Dropdown-Liste **Schriftarten für Berichte** können Sie eine Schriftart auswählen, die beim PDF-Export der Berichte verwendet wird.
- Im Feld **Größe der Schriftart für Berichte** wird die Schriftgröße für den allgemeinen Text in Statistiktabellen festgelegt. Diese Schriftgröße wird beim PDF-Export der Berichte verwendet.

Berichte

In diesem Unterbereich wird die Anzeige von statistischen Daten im Bereich **Berichte** des **Verwaltungscenters** eingestellt:

- Im Feld **Zeilenanzahl pro Seite** wird die maximale Anzahl von Zeilen auf einer Seite des Berichts bei der Einzelseitenansicht von Statistiken festgelegt.
- Aktivieren Sie das Kontrollkästchen **Diagramme anzeigen**, um Diagramme in den Statistikberichten anzeigen zu lassen. Beim deaktivierten Kontrollkästchen wird die Anzeige von Diagrammen deaktiviert.

Abonnement

In diesem Unterbereich können Sie Nachrichten von **Doctor Web** abonnieren.

Aktivieren Sie das Kontrollkästchen **Automatisches Abonnement für neue Bereiche**, damit automatisch neue Abschnitte für Nachrichten im **Verwaltungscenter** hinzugefügt werden.

2.3.5. Hilfe

Um zum Hilfebereich des **Verwaltungscenters** zu wechseln, klicken Sie im Hauptmenü auf .

Das Verwaltungsmenü im linken Fensterbereich enthält die folgenden Elemente:

1. **Allgemein**
   - **Forum**. Öffnet die Foren-Webseite von **Doctor Web**.
   - **News**. Öffnet die Seite mit Unternehmensnachrichten von **Doctor Web**.
   - **Kontakt zum technischen Support**. Öffnet das **Support**-Portal von **Doctor Web**.
   - **Verdächtige Datei einsenden**. Öffnet den Abschnitt, in dem Sie eine vermutlich infizierte Datei an das Virenlabor von **Doctor Web** senden können.
   - **Doctor Web-Wikipedia**. Öffnet das Wiki-Portal zu Produkten von **Doctor Web**.
   - **Fehlalarm von Office Control Control melden**. Öffnet das Formular zum Versand von Nachrichten über Fehlalarme oder Erkennungsfehler im Modul **Office Control Control**.
2. **Administratordokumentation**
   - **Administratorhandbuch**. Öffnet das Administratorhandbuch im HTML-Format.
   - **Installationsanleitung**. Öffnet die Installationsanleitung für **Dr.Web Enterprise Security Suite** im HTML-Format.
   - **Anhänge**. Öffnet die Anhänge zum Administratorhandbuch im HTML-Format.
   - **Anleitung für Web API**. Öffnet die Administratoranleitung für Web API (s. auch das Dokument **Anhänge** unter Anhang L. Integration von Web API und Dr.Web Enterprise Security Suite) im HTML-Format.
   - **Anmerkungen zu dieser Version**. Öffnet den Bereich mit Anmerkungen zur installierten Version von **Dr.Web Enterprise Security Suite**.
3. **Benutzerdokumentation**. Enthält Benutzerhandbücher im HTML-Format für aufgelistete Betriebssysteme.

2.4. Komponenten des Dr.Web Sicherheitscenters

2.4.1. Netzwerk-Scanner

Zum Leistungsumfang des **Dr.Web Servers** gehört der **Netzwerk-Scanner**.

Falls möglich, vermeiden Sie die Verwendung des **Netzwerk-Scanners** unter Windows 2000 oder früher. Bei diesen Betriebssystemen kann die Übersicht des Netzwerks nicht vollständig sein.

Ein sicherer Betrieb des **Netzwerk-Scanners** kann nur unter Betriebssystemen der UNIX-Familie bzw. unter Windows XP oder neuer garantiert werden.

Um den **Netzwerk-Scanner** verwenden zu können, müssen Sie die Browser-Erweiterung für das **Dr.Web Sicherheitscenter** installieren.

Damit der **Netzwerk-Scanner** im Webbrowser Windows Internet Explorer korrekt angezeigt wird, sollte die Adresse des **Verwaltungscenters**, in dem der **Netzwerk-Scanner** gestartet wird, zur Liste der vertrauenswürdigen Webseiten des Webbrowsers hinzugefügt werden: **Tools** (**Extras**) → **Internet Options** (**Internetoptionen**) → **Security** (**Sicherheit**) → **Trusted Sites** (**Vertrauenswürdige Sites**).

Der Netzwerk-Scanner hat die folgenden Leistungsmerkmale:

- Scannen (Durchsuchen) des Netzwerks nach Workstations.
- Suche nach installierten **Dr.Web Agents**.
- Installation des **Dr.Web Agents** auf gefundenen Workstations durch den Administrator. Die Installation des **Dr.Web Agents** wird in der **Installationsanleitung** unter Dr.Web Agent über das Sicherheitscenter installieren detailliert beschrieben.

So scannen (durchsuchen) Sie das Netzwerk

1. Öffnen Sie den **Netzwerk-Scanner**. Wählen Sie hierzu im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster den Menü **Netzwerk-Scanner**. Es öffnet sich das Fenster **Netzwerk-Scanner**.
2. Aktivieren Sie das Kontrollkästchen **Suche nach IP-Adressen**, um im Netzwerk nach Workstations innerhalb des angegebenen IP-Adressbereiches zu suchen. Im Eingabefeld **Netzwerke** geben Sie den gewünschten IP-Adressbereich wie folgt ein:
   - Durch einen Bindestrich getrennt (z.B. `10.4.0.1-10.4.0.10`).
   - Durch ein Komma und Leerzeichen getrennt (z. B. `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`).
   - Durch Angabe eines Netzwerkpräfixes (z.B. `10.4.0.0/24`).
3. Aktivieren Sie unter Windows das Kontrollkästchen **In Active Directory suchen**, um nach Workstations in der Active Directory-Domäne zu suchen. Legen Sie die folgenden Parameter fest:
   - **Domänen** – ist die Liste der Domänen, in denen es nach Workstations gesucht wird. Verwenden Sie das Komma-Zeichen, um mehrere Domänen voneinander zu trennen.
   - **Active Directory-Controller** – ist der Active Directory Controller , z.B. dc.example.com.

   Um nach Workstations in einer Active Directory-Domäne über den **Netzwerk-Scanner** zu suchen, muss der Webbrowser, in dem das **Verwaltungscenter** geöffnet ist, unter dem Domänenbenutzerkonto ausgeführt werden, das über die Berechtigung zur Suche nach Active Directory-Objekten verfügt.
4. Bei UNIX-ähnlichen Betriebssystemen: Aktivieren Sie das Kontrollkästchen **Nach LDAP suchen**, um nach Workstations über LDAP zu suchen. Legen Sie die folgenden Parameter fest:
   - **Domänen** – ist die Liste der Domänen, in denen es nach Workstations gesucht wird. Verwenden Sie das Komma-Zeichen, um mehrere Domänen voneinander zu trennen.
   - **LDAP-Server** – ist ein LDAP-Server, zum Beispiel ldap://ldap.example.com.
   - **Anmeldename** – ist der Anmeldename des LDAP-Benutzers.
   - **Passwort** – ist das Passwort des LDAP-Benutzers.
5. Geben im Feld **Port** die Portnummer ein, die bei der Suche für die UDP-Verbindung mit den **Agents** verwendet wird.
6. Ändern Sie bei Bedarf im Feld **Timeout (Sek.)** den definierten Wert für das Zeitlimit in Sekunden, innerhalb dessen eine Antwort von den abgefragten Workstations erwartet wird.
7. Aktivieren Sie das Kontrollkästchen **Schnelles Scannen**, um einen Schnell-Scan durchzuführen.
8. Aktivieren Sie das Kontrollkästchen **Namen der Workstations anzeigen**, um für die gefundenen Rechner nicht nur ihre IP-Adresse, sondern auch ihre DNS-Namen anzeigen zu lassen.

Wenn eine Workstation auf dem DNS-Server nicht registriert ist, wird nur ihre IP-Adresse angezeigt.

9. Aktivieren Sie das Kontrollkästchen **Workstations-Liste aus der Datenbank zuordnen**, damit Suchergebnisse des **Netzwerk-Scanners** mit der in der Datenbank des **Servers** gespeicherten Liste von Workstations synchronisiert werden. Wenn dieses Kontrollkästchen aktiviert ist, werden in der Liste der gefundenen Workstations auch die Workstations angezeigt, die zwar in der Datenbank des **Servers** vorhanden sind, aber bei der Suche durch den **Netzwerk-Scanner** nicht erkannt wurden. Das passiert beispielsweise dann, wenn auf der Workstation eine Firewall installiert ist, der bei der Herstellung einer TCP-Verbindung die Paketübertragung blockiert.

   Bei der Synchronisierung von Suchergebnissen des **Netzwerk-Scanners** mit den Daten aus der Datenbank des **Servers** haben die Daten aus der Datenbank des **Servers** eine höhere Priorität: Wenn der Status einer Workstation in den Suchergebnissen nicht mit dem in der Datenbank gespeicherten Status übereinstimmt, wird also der in der Datenbank gespeicherte Status festgelegt.

10. Klicken Sie auf **Scannen**, um das Netzwerk zu durchsuchen.
11. Beim Durchsuchen wird im Fenster ein Verzeichnis (eine hierarchische Liste) der Rechner geladen. Bei jedem Rechner wird dabei angegeben, ob er über den installierten **Dr.Web Agent** verfügt.

    Erweitern Sie die Elemente des Verzeichnisses, die den Arbeitsgruppen (Domänen) entsprechen. Alle Elemente des Verzeichnisses, die den Arbeitsgruppen und einzelnen Workstations entsprechen, werden durch unterschiedliche Symbole markiert. Ihre jeweilige Bedeutung finden Sie in der Tabelle unten.

Tabelle 2-2: Mögliche Symbole

Symbol	Erläuterung
	Arbeitsgruppen
	Arbeitsgruppen, zu denen u. a. die Rechner gehören, auf denen **Dr.Web Enterprise Security Suite** installiert werden kann.
	Sonstige Gruppen, zu denen Rechner mit bereits installierter Antivirensoftware bzw. im Netzwerk nicht verfügbare Rechner gehören.
	Workstations
	Die gefundene Workstation ist in der Datenbank registriert und aktiv (aktive Workstations mit der installierten Antivirensoftware).
	Die gefundene Workstation ist in der Datenbank, in der Tabelle der gelöschten Workstations registriert.
	Die gefundene Workstation ist in der Datenbank nicht registriert (auf dem Rechner ist keine Antivirensoftware vorhanden).
	Die gefundene Workstation ist in der Datenbank nicht registriert (die Workstation ist mit einem anderen **Server** verbunden).
	Die gefundene Workstation ist in der Datenbank zwar registriert, ist aber nicht aktiv, und der Port ist geschlossen.

Die Verzeichniselemente, die den Workstations mit dem Symbol oder entsprechen, können erweitert werden. Dabei können Sie auch die darauf installierten Komponenten einsehen.

Interaktion mit Dr.Web Agents

Der **Netzwerk-Scanner** gehört zum Leistungsumfang von **Dr.Web Enterprise Security Suite** erst ab Version **4.44**.

Der **Netzwerk-Scanner** erkennt daher nur die **Agents** der Version **4.44** oder höher. Das Interagieren mit den **Agents** früherer Versionen ist nicht möglich.

Der auf einer Workstation installierte **Agent** der Version **4.44** oder höher verarbeitet die entsprechenden Anforderungen des **Netzwerk-Scanners**, die an einem bestimmten Port empfangen werden. Standardmäßig wird der Port `udp/2193` verwendet. Um die Kompatibilität mit der Software von früheren Versionen sicherzustellen, wird auch der Port `udp/2372` unterstützt. Diese Ports werden standardmäßig im **Netzwerk-Scanner** abgefragt. Der **Netzwerk-Scanner** entscheidet nach dem Anfrage-Antwort Prinzip, ob der **Agent** auf der Workstation vorhanden ist, indem er über den genannten Port eine Anfrage sendet und eventuell eine Rückbestätigung empfängt.

Wenn auf der Workstation der Empfang von Paketen am Port `udp/2193` nicht möglich ist (z.B. werden Pakete von der installierten Firewall abgewiesen), kann der **Agent** nicht erkannt werden. Der **Agent** gilt in diesem Fall für den **Netzwerk-Scanner** als nicht installiert.

Schnelles Scannen

Bei der aktivierten Option **Schnelles Scannen** werden die folgenden Aktionen ausgeführt:

1. An die Rechner des Netzwerks werden Ping-Anforderungen gesendet.
2. Rechner, die auf die Ping-Anforderung geantwortet haben, werden parallel auf installierte **Agents** überprüft.
3. Das Verfahren zur Erkennung eines installierten **Agents** wird nach allgemeinen Regeln ausgeführt.

Ping-Anforderungen können aufgrund der definierten Netzwerkrichtlinien (z.B. aufgrund der Firewall-Einstellungen) abgewiesen werden.

Beispiel:

Wenn in den Netzwerkeinstellungen von Windows Vista oder neuer die Option **Öffentliches Netzwerk** gewählt wurde, werden eingehende Ping-Anforderungen vom Betriebssystem blockiert.

Beim Standard-Scan werden keine Ping-Anforderungen versendet. Stattdessen werden alle Workstations auf einen installierten **Agent** der Reihe nach überprüft. Dieses Verfahren kann zusätzlich zum Schnell-Scan in dem Fall verwendet werden, wenn es innerhalb des Netzwerks Workstations gibt, auf denen keine Ping-Anforderungen empfangen werden können.

Der Schnell-Scan wird parallel ausgeführt. Der Standard-Scan erfolgt sequentiell.

Die Dauer des Scans durch den **Netzwerk-Scanner** ist jeweils nicht identisch. Die maximale Scandauer bei jedem Scan-Modus wird wie folgt berechnet:

- Beim Standard-Scan: *<N>* * *<timeout>*.
- Beim schnellen Scan: *<N>*/40 + 2**<timeout>*.

Dabei gilt das Folgende:*<N>* ist die Anzahl von Workstations, *<timeout>* ist der Wert im Feld **Timeout**.

2.4.2. Lizenzmanager

Besonderheiten der Lizenzierung

1. Der **Dr.Web Server** wird nicht lizenziert. Bei der Installation des **Servers** können Sie keinen Lizenzschlüssel angeben. Ein gültiger Lizenzschlüssel kann nachträglich sowohl lokal, als auch über die Server-zu-Server-Kommunikation hinzugefügt werden.

UUID des **Servers**, die in früheren Versionen von **Dr.Web Enterprise Security Suite** im Lizenzschlüssel des **Servers** gespeichert wurde, wird ab Version **10.0** in der Konfigurationsdatei des **Servers** gespeichert.

- Bei der Installation eines neuen **Servers** wird eine neue UUID generiert.
- Beim Upgrade des **Servers** von einer früheren Version, wird die UUID aus dem Schlüssel des **Servers** der früheren Version (Datei `enterprise.key` im Verzeichnis `etc` der vorherigen Installation des **Servers**) automatisch übernommen und in die Konfigurationsdatei des zu installierenden **Servers** geschrieben.

Beim Upgrade des Clusters der **Server** erhält nur der für die Aktualisierung von Datenbanken zuständige **Server** einen Lizenzschlüssel. Bei den anderen **Servern** sollten Lizenzschlüssel manuell hinzugefügt werden

2. Lizenzschlüssel gelten jeweils nur für die geschützten Workstations. Schlüsseldateien können hingegen sowohl einzelnen Workstations, als auch Gruppen von Workstations zugewiesen werden. Im letzteren Fall gilt ein Lizenzschlüssel für alle Workstations, die ihn von der Gruppe erben. Um eine Schlüsseldatei gleichzeitig allen Workstations, für die keine individuellen Einstellungen des Lizenzschlüssels festgelegt wurden, zuzuweisen, weisen Sie den vorhandenen Lizenzschlüssel der Gruppe **Everyone** zu.
3. Über die Server-zu-Server-Kommunikation kann eine optionale Anzahl der Lizenzen aus den Schlüsseln, die auf diesem **Server** gespeichert sind, auf einen benachbarten **Server** für einen bestimmten Zeitraum übertragen werden.
4. Jeder Lizenzschlüssel kann gleichzeitig mehreren Objekten (Gruppen und Workstations) zugewiesen werden. Einem lizenzierten Objekt kann gleichzeitig mehrere Lizenzschlüssel zugewiesen werden.
5. Wenn einem Objekt mehrere Schlüssel zugewiesen werden, achten Sie auf das Folgende:
   a) Wenn die Listen erlaubter Antivirenkomponenten in einigen Schlüsseln eines Objekts nicht identisch sind, wird die Liste der für die Workstation erlaubten Antivirenkomponenten anhand der Schnittmenge von Komponenten in den Schlüsseln definiert. Zum Beispiel, wenn einer Workstation ein Schlüssel mit der **Antispam**-Komponente und ein Schlüssel ohne **Antispam**-Komponente zugewiesen werden, kann auf der Workstation die **Antispam**-Komponente nicht installiert werden.
   b) Die Lizenzierungseinstellungen für das Objekt werden anhand aller dem Objekt zugewiesenen Schlüssel berechnet. Wenn die Lizenzschlüssel des Objekts nicht die gleiche Gültigkeitsdauer haben, müssen Sie nach Ablauf des Lizenzschlüssels mit der kürzesten Gültigkeitsdauer den abgelaufenen Schlüssel erneuern oder manuell entfernen. Wenn sich der abgelaufene Schlüssel nur auf bestimmte Komponenten beschränkte, müssen Sie im Bereich Installierte Komponenten die Einstellungen des lizenzierten Objekts entsprechend anpassen.
   c) Die Anzahl der Lizenzen eines Objekts wird anhand der Summe von Lizenzen aller Schlüssel berechnet, die dem Objekt zugewiesen wurden. Beim Berechnen müssen die Lizenzen berücksichtigt werden, die eventuell auf einen benachbarten **Server** (s. den Punkt 3) über die Server-zu-Server-Kommunikation übertragen werden. Die dadurch auf den benachbarten **Server** übertragenen Lizenzen müssen dann von der Gesamtzahl der Lizenzen abgezogen werden.

Die den Lizenzschlüssel enthaltene Datei wird bei der Installation des **Dr.Web Servers** angegeben (mehr dazu finden Sie in der **Installationsanleitung** unter Dr.Web Server installieren). Nachträglich können Sie neue Schlüssel erhalten, z. B. mit einer längeren Lizenz-Gültigkeitsdauer oder einem anderen Komponentensatz.

Jede Schlüsseldatei wird durch eine digitale Signatur vor unbefugten Änderungen geschützt. Durch eventuelle Bearbeitung wird die Datei nicht mehr gültig. Um eine zufällige Beschädigung der Datei zu vermeiden, dürfen Sie Ihre Schlüsseldatei nicht bearbeiten und/oder nach dem Öffnen in einem Texteditor speichern.

Benutzeroberfläche des Lizenzmanagers

Zum Leistungsumfang des **Verwaltungscenters** gehört der **Lizenzmanager**. Diese Komponente wird zur Lizenzierung der Objekte des Antivirus-Netzwerks verwendet.

Um das Fenster des **Lizenzmanagers** aufzurufen, wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im danach erschienenen Fenster den Punkt des Verwaltungsmenüs **Lizenzmanager**.

Hierarchische Liste der Schlüssel

Das Hauptfenster des **Lizenzmanagers** enthält eine Schlüsselstruktur, d. h. eine hierarchische Liste, deren Knoten Lizenzschlüssel, Workstations und Gruppen mit zugewiesenen Schlüsseln bilden.

Die Symbolleiste enthält die folgenden Elemente:

Option	Erläuterung	Abhängigkeit von den Objekten in der Schlüsselstruktur
Schlüssel hinzufügen	Neuen Lizenzschlüssel-Datensatz hinzufügen.	Die Option ist immer verfügbar. Funktionen hängen davon ab, ob ein Objekt in der Schlüsselstruktur gewählt ist (s. Neuen Lizenzschlüssel hinzufügen).
Ausgewählte Objekte entfernen	Das lizenzierte Objekt vom Schlüssel trennen.	Die Option ist nur dann verfügbar, wenn in der Schlüsselstruktur ein lizenziertes Objekt (Workstation oder Gruppe) bzw. ein Lizenzschlüssel gewählt ist.
Den Schlüssel auf Gruppen und Workstations verbreiten	Den gewählten Schlüssen ersetzen oder einem lizenzierten Objekt hinzufügen.	Die Option ist nur dann verfügbar, wenn in der Schlüsselstruktur ein Lizenzschlüssel gewählt ist.
Schlüssel exportieren	Eine lokale Kopie der Datei des Lizenzschlüssels speichern.	
Den Schlüssel auf Nachbarserver verbreiten	Lizenzen aus dem gewählten Schlüssel auf benachbarte **Server** verteilen.	

Einstellungen der Verzeichnisstruktur. Durch diese Option kann die Strukturansicht angepasst werden.

- Das Kontrollkästchen **Anzahl der Lizenzen anzeigen** aktiviert bzw. deaktiviert die Anzeige der Gesamtanzahl der Lizenzen, die Schlüsseldateien bereitstellen.
- Zum Ändern der Struktur verwenden Sie die folgenden Optionen:
  - Die Option **Schlüssel** gibt an, dass alle Lizenzschlüssel des Antivirus-Netzwerks als Knoten der Schlüsselstruktur angezeigt werden sollen. Dabei werden alle Gruppen und Workstations, denen diese Lizenzschlüssel zugewiesen wurden, als untergeordnete Elemente angezeigt. Diese Strukturansicht ist die allgemeine Ansicht, die zur Verwaltung der lizenzierten Objekte und Lizenzschlüssel dient.
  - Die Option **Gruppen** gibt an, dass als Knoten der hierarchischen Struktur diejenigen Gruppen angezeigt werden sollen, denen die Lizenzschlüssel direkt zugewiesen wurden. Dabei werden Workstations, die diesen Gruppen angehören, und Lizenzschlüssel, die diesen Gruppen zugewiesen wurden, als untergeordnete Elemente angezeigt. Diese Ansicht dient lediglich zum bequemen Darstellen der Informationen über die Lizenzierung und lässt keine Objekte verwalten.

Lizenzen verwalten

Der Lizenzmanager ermöglicht die folgenden Aktionen mit Lizenzschlüsseln des Dr.Web Servers:

1. Informationen zur Lizenz anzeigen.

2. Neuen Lizenzschlüssel hinzufügen.
3. Lizenzschlüssel aktualisieren.
4. Lizenzschlüssel ersetzen.
5. Liste der Lizenzschlüssel des Objekts erweitern.
6. Lizenzschlüssel und Objekt aus der Liste der lizenzierten Objekte entfernen.
7. Lizenzen auf benachbarte Server verteilen.
8. Lizenzen auf benachbarten Servern bearbeiten.

Informationen zur Lizenz anzeigen

Um die Übersichtsinformationen zu einem Lizenzschlüssel einzusehen, wählen Sie im Hauptfenster des **Lizenzmanagers** den Datensatz des gewünschten Schlüssels. Klicken Sie dafür auf den Datensatz des Schlüssels. Im danach erschienenen Fenster werden die folgenden Informationen angezeigt:

- Lizenzinhaber;
- Verkäufer der Lizenz;
- ID und Seriennummer der Lizenz;
- Ablaufdatum der Lizenz;
- Verfügbarkeit der **Antispam**-Komponente;
- Anzahl der durch diese Schlüsseldatei lizenzierten Workstations;
- MD5-Hashwert des Lizenzschlüssels;
- Liste der Antivirenkomponenten, die zum Lizenzumfang gehören.

Neuen Lizenzschlüssel hinzufügen

So fügen Sie einen neuen Lizenzschlüssel hinzu

1. Klicken Sie im Hauptfenster des **Lizenzmanagers** die Schaltfläche **Schlüssel hinzufügen** an, die sich in der Symbolleiste befindet.
2. Klicken Sie im geöffneten Fenster auf und wählen Sie die gewünschte Lizenzschlüssel-Datei.
3. Klicken Sie auf **Speichern**.
4. Der Lizenzschlüssel wird zur Schlüsselstruktur zwar hinzugefügt, doch wird er keinem Objekt zugewiesen. In diesem Fall müssen Sie zum Festlegen der zu lizenzierenden Objekte die unten beschriebenen Aktionen Lizenzschlüssel ersetzen oder Liste der Lizenzschlüssel des Objekts erweitern ausführen.

Lizenzschlüssel aktualisieren

Bei der Aktualisierung eines Lizenzschlüssels wird der neue Lizenzschlüssel den gleichen lizenzierten Objekten zugewiesen, denen der aktualisierte Schlüssel zugewiesen wurde.

Verwenden Sie diese Aktion, um einen abgelaufenen Lizenzschlüssel zu ersetzen oder ihn durch einen Lizenzschlüssel mit anderen Komponenten zu ersetzen und dabei die vorhandene Schlüsselstruktur zu erhalten.

So aktualisieren Sie einen Lizenzschlüssel

1. Wählen Sie im Hauptfenster des **Lizenzmanagers** in der Schlüsselstruktur den zu aktualisierenden Schlüssel.
2. Klicken Sie im geöffneten Fenster der Schlüsseleigenschaften auf und wählen Sie die gewünschte Lizenzschlüssel-Datei.

3. Klicken Sie auf **Speichern**. Es öffnet sich das Fenster mit den Einstellungen der zu installierenden Komponenten, das unter Einstellungen zum Ersetzen eines Lizenzschlüssels detailliert beschrieben wird.
4. Klicken Sie auf **Speichern**, um den Lizenzschlüssel zu aktualisieren.

Lizenzschlüssel ersetzen

Beim Ersetzen eines Lizenzschlüssels werden alle aktuellen Lizenzschlüssel des lizenzierten Objekts entfernt, und ein neuer Lizenzschlüssel wird diesem Objekt hinzugefügt.

So ersetzen Sie den aktuellen Lizenzschlüssel

1. Wählen Sie im Hauptfenster des **Lizenzmanagers** in der Schlüsselstruktur einen Schlüssel, den Sie dem lizenzierten Objekt zuweisen möchten.
2. Klicken Sie auf der Symbolleiste auf **Den Schlüssel auf Gruppen und Workstations verbreiten**. Es öffnet sich das Fenster mit der hierarchischen Liste von Workstations und Gruppen des Antivirus-Netzwerks.
3. Wählen Sie in der Liste das gewünschte lizenzierte Objekt. Eine Mehrfachauswahl ist mit gedrückter STRG- und UMSCHALTTASTE möglich.
4. Klicken Sie auf **Schlüssel ersetzen**. Es öffnet sich das Fenster mit den Einstellungen der zu installierenden Komponenten, das unter Einstellungen zum Ersetzen eines Lizenzschlüssels detailliert beschrieben wird.
5. Klicken Sie auf **Speichern**, um den Lizenzschlüssel zu ersetzen.

Liste der Lizenzschlüssel des Objekts erweitern

Beim Hinzufügen eines Lizenzschlüssels bleiben alle aktuellen Lizenzschlüssel des lizenzierten Objekts erhalten, und ein neuer Lizenzschlüssel wird der Liste der Lizenzschlüssel hinzugefügt.

So fügen Sie der Liste der Lizenzschlüssel einen neuen Lizenzschlüssel hinzu

1. Wählen Sie im Hauptfenster des **Lizenzmanagers** in der Schlüsselstruktur einen Schlüssel, den Sie zur Liste der Schlüssel des Objekts hinzufügen möchten.
2. Klicken Sie auf der Symbolleiste auf **Den Schlüssel auf Gruppen und Workstations verbreiten**. Es öffnet sich das Fenster mit der hierarchischen Liste von Workstations und Gruppen des Antivirus-Netzwerks.
3. Wählen Sie in der Liste das gewünschte lizenzierte Objekt. Eine Mehrfachauswahl ist mit gedrückter STRG- und UMSCHALTTASTE möglich.
4. Klicken Sie auf **Schlüssel hinzufügen**. Es öffnet sich das Fenster mit den Einstellungen der zu installierenden Komponenten, das unter Einstellungen zum Hinzufügen eines Lizenzschlüssels zur Liste der Schlüssel detailliert beschrieben wird.
5. Klicken Sie auf **Speichern**, um den Lizenzschlüssel hinzuzufügen.

Lizenzschlüssel und Objekt aus der Liste der lizenzierten Objekte entfernen.

Der letzte Datensatz des Schlüssels der Gruppe **Everyone** kann nicht entfernt werden.

So entfernen Sie einen Lizenzschlüssel oder ein Objekt aus der Liste der lizenzierten Objekte

1. Wählen Sie im Hauptfenster des **Lizenzmanagers** den Schlüssel, den Sie entfernen möchten, bzw. das Objekt (Workstation oder Gruppe), dem dieser Schlüssel zugewiesen wurde, und klicken Sie in der Symbolleiste auf **Ausgewählte Objekte entfernen**. Beachten Sie dabei das Folgende:
   - Wenn Sie ein lizenziertes Objekt ausgewählt haben, wird es aus der Liste der Objekte entfernt, für die der ihm zugewiesene Schlüssel gilt. Das Objekt, bei dem sein individueller Schlüssel entfernt wird, erbt den Lizenzschlüssel.
   - Wenn Sie einen Lizenzschlüssel ausgewählt haben, wird der Datensatz des Schlüssels aus dem Antivirus-Netzwerk entfernt. Alle Objekte, denen dieser Schlüssel zugewiesen wurde, erben den Lizenzschlüssel.
2. Es öffnet sich das Fenster mit den Einstellungen der zu installierenden Komponenten, das unter Einstellungen zum Ersetzen eines Lizenzschlüssels detailliert beschrieben wird.
3. Klicken Sie auf **Speichern**, um den gewählten Schlüssel zu entfernen und auf den geerbten Schlüssel umzuschalten.

Lizenzen auf benachbarte Server verteilen

Wenn eine Anzahl der im Lizenzschlüssel dieses **Servers** enthaltenen freien Lizenzen auf einen benachbarten **Server** verteilt wird, können die verteilten Lizenzen auf diesem **Server** innerhalb des gesamten Verteilungszeitraums nicht verwendet werden.

So verteilen Sie Lizenzen auf benachbarte Server

1. Wählen Sie im Hauptfenster des **Lizenzmanagers** in der Schlüsselstruktur den Schlüssel, dessen freie Lizenzen Sie auf einen benachbarten **Server** verteilen möchten.
2. Klicken Sie auf der Symbolleiste auf **Den Schlüssel auf Nachbarserver verbreiten**. Es öffnet sich das Fenster mit der hierarchischen Liste von benachbarten **Servern**.
3. Wählen Sie in der Liste die **Server**, auf die Sie Lizenzen verteilen möchten.
4. Legen Sie bei jedem **Server** die folgenden Einstellungen fest:
   - **Anzahl der Lizenzen**. Hier wird die Anzahl der im Schlüssel enthaltenen freien Lizenzen angegeben, die Sie auf den benachbarten **Server** verteilen möchten.
   - **Datum des Lizenzablaufs**. Hier wird der Verteilungszeitraum angegeben. Nach Ablauf des Zeitraums werden alle Lizenzen vom benachbarten **Server** zurückgerufen und zur Liste der freien Lizenzen dieses Lizenzschlüssels hinzugefügt.
5. Klicken Sie eine der folgenden Schaltflächen an:
   - **Schlüssel hinzufügen**. Dadurch fügen Sie Lizenzen zur Liste der vorhandenen Lizenzen auf den benachbarten **Servern** hinzu. Es öffnet sich das Fenster mit den Einstellungen der zu installierenden Komponenten, das unter Einstellungen zum Hinzufügen eines Lizenzschlüssels zur Liste der Schlüssel detailliert beschrieben wird.
   - **Schlüssel ersetzen**. Dadurch entfernen Sie die vorhandenen Lizenzen auf benachbarten **Servern** und legen nur die zu verteilenden Lizenzen fest. Es öffnet sich das Fenster mit den Einstellungen der zu installierenden Komponenten, das unter Einstellungen zum Ersetzen eines Lizenzschlüssels detailliert beschrieben wird.
6. Klicken Sie auf **Speichern**, um Lizenzen auf die benachbarten **Server** zu verteilen.

Lizenzen auf benachbarten Servern bearbeiten

So bearbeiten Sie Lizenzen auf benachbarten Servern

1. Wählen Sie im Hauptfenster des **Lizenzmanagers** in der Schlüsselstruktur den benachbarten **Server**, auf den Lizenzen verteilt wurden.
2. Passen Sie im geöffneten Eigenschaftenfenster die folgenden Einstellungen an:

- **Anzahl der Lizenzen**. Hier wird die Anzahl der freien Lizenzen angegeben, die vom Schlüssel dieses **Servers** auf den benachbarten **Server** verteilt wurden.
- **Datum des Lizenzablaufs**. Hier wird der Verteilungszeitraum angegeben. Nach Ablauf des Zeitraums werden alle Lizenzen vom benachbarten **Server** zurückgerufen und zur Liste der freien Lizenzen des aktuellen Lizenzschlüssels hinzugefügt.

3. Klicken Sie auf **Speichern**, um die Informationen über die zu verteilenden Lizenzschlüssel zu aktualisieren.

Änderungen an der Liste der zu installierenden Komponenten vornehmen

Einstellungen zum Ersetzen eines Lizenzschlüssels

Hier werden die Einstellungen der zu installierenden Komponenten beschrieben, die bei der Ausführung der folgenden Aktionen verwendet werden:

- Lizenzschlüssel aktualisieren.
- Lizenzschlüssel ersetzen.
- Lizenzschlüssel entfernen.
- Lizenzen auf benachbarte **Server** verteilen und Schlüssel ersetzen.

So stellen Sie die zu installierenden Komponenten bei der Ausführung dieser Aktionen ein

1. Im Eigenschaftenfenster der zu installierenden Komponenten werden die folgenden Objekte aufgeführt:
   - Workstations und Gruppen mit den eigenen Listen der zu installierenden Komponenten.
   - In der Spalte **Aktueller Schlüssel** wird die Liste der Schlüssel des Objekts und der Einstellungen der zu installierenden Komponenten angezeigt, die für das Objekt zurzeit aktuell sind.
   - In der Spalte **Importierter Schlüssel** werden der Schlüssel und die Einstellungen der zu installierenden Komponenten angezeigt, die im Schlüssel festgelegt wurden, der den gewählten Objekten zugewiesen werden soll.
2. Aktivieren Sie bei Bedarf das Kontrollkästchen **Nur bei Unterschied anzeigen**, um in der Liste nur diejenigen Komponenten anzeigen zu lassen, deren Einstellungen im aktuellen Schlüssel und importierten Schlüssel nicht identisch sind.
3. Um die Liste der zu installierenden Komponenten zu konfigurieren, gehen Sie so vor:

   a) In der Spalte **Importierter Schlüssel** können Sie die resultierende Liste der zu installierenden Komponenten konfigurieren.

   - Die Einstellungen der zu installierenden Komponenten in der Spalte **Importierter Schlüssel** hängen davon ab, ob die aktuellen Einstellungen und Einstellungen des importierten Schlüssels die Verwendung der jeweiligen Komponente zulassen (+) oder nicht (–).

Aktuelle Einstellungen	Einstellungen des importierten Schlüssels	Resultierende Einstellungen
+	+	+
–	+	+
+	–	–
–	–	–

   - Sie können die Einstellungen der zu installierenden Komponenten nur dann ändern (niedrigere Rechte für die Installation zuweisen), wenn die resultierenden Einstellungen in der Spalte **Importierter Schlüssel** die Verwendung dieser Komponente zulassen.

b) Aktivieren Sie die Kontrollkästchen neben denjenigen Objekten (Workstations und Gruppen), für welche die Vererbung der Einstellungen unterbrochen wird und die Einstellungen der zu installierenden Komponenten aus der Spalte **Importierter Schlüssel** als individuelle Einstellungen übernommen werden. Für die anderen Objekte (mit deaktivierten Kontrollkästchen) werden die ursprünglichen Einstellungen aus der Spalte **Importierter Schlüssel** geerbt.

Einstellungen zum Hinzufügen eines Lizenzschlüssels zur Liste der Schlüssel

Hier werden die Einstellungen der zu installierenden Komponenten beschrieben, die bei der Ausführung der folgenden Aktionen verwendet werden:

- Liste der Lizenzschlüssel des Objekts erweitern.
- Lizenzen auf benachbarte **Server** verteilen und Schlüssel hinzufügen.

So stellen Sie die zu installierenden Komponenten bei der Ausführung dieser Aktionen ein

1. Im Eigenschaftenfenster der zu installierenden Komponenten werden die folgenden Objekte aufgeführt:
   - Workstations und Gruppen mit den eigenen Listen der zu installierenden Komponenten.
   - In der Spalte **Aktueller Schlüssel** wird die Liste der Schlüssel des Objekts und der Einstellungen der zu installierenden Komponenten angezeigt, die für das Objekt zurzeit aktuell sind.
   - In der Spalte **Importierter Schlüssel** werden der Schlüssel und die Einstellungen der zu installierenden Komponenten angezeigt, die im Schlüssel festgelegt wurden, den Sie zu den gewählten Objekten hinzufügen möchten.
2. Aktivieren Sie bei Bedarf das Kontrollkästchen **Nur bei Unterschied anzeigen**, um in der Liste nur diejenigen Komponenten anzeigen zu lassen, deren Einstellungen im aktuellen Schlüssel und importierten Schlüssel nicht identisch sind. Beachten Sie dabei, dass unter **Importierter Schlüssel** nicht die Einstellungen des importierten Schlüssels, sondern die resultierenden Einstellungen der zu installierenden Komponenten aufgeführt werden.
3. Um die Liste der zu installierenden Komponenten zu konfigurieren, gehen Sie so vor:

   a) In der Spalte **Importierter Schlüssel** können Sie die resultierende Liste der zu installierenden Komponenten konfigurieren.

   - Die Einstellungen der zu installierenden Komponenten in der Spalte **Importierter Schlüssel** hängen davon ab, ob die aktuellen Einstellungen und Einstellungen des importierten Schlüssels die Verwendung der jeweiligen Komponente zulassen (+) oder nicht (–).

Aktuelle Einstellungen	Einstellungen des importierten Schlüssels	Resultierende Einstellungen
+	+	+
–	+	–
+	–	–
–	–	–

   - Sie können die Einstellungen der zu installierenden Komponenten nur dann ändern (niedrigere Rechte für die Installation zuweisen), wenn die resultierenden Einstellungen in der Spalte **Importierter Schlüssel** die Verwendung dieser Komponente zulassen.

   b) Aktivieren Sie die Kontrollkästchen neben denjenigen Objekten (Workstations und Gruppen), für welche die Vererbung der Einstellungen unterbrochen wird und die Einstellungen der zu installierenden Komponenten aus der Spalte **Importierter Schlüssel** als individuelle Einstellungen übernommen werden. Für die anderen Objekte (mit deaktivierten Kontrollkästchen) werden die Einstellungen aus der Spalte **Importierter Schlüssel** geerbt.

2.5. Zusammenwirken von Komponenten des Antivirus-Netzwerks

Die Abbildung 2-2 zeigt ein allgemeines Schema des Antivirus-Netzwerks.

Auf dem Schema ist ein Antivirus-Netzwerk dargestellt, das nur aus einem **Server** besteht. Wenn möglich, sollte in großen Unternehmen ein Antivirus-Netzwerk mit mehreren **Servern** eingerichtet werden. Dadurch kann die Last gleichmäßig auf die Server verteilt werden.

In diesem Beispiel ist das Antivirus-Netzwerk innerhalb eines lokalen Netzwerks eingerichtet. Um **Dr.Web Enterprise Security Suite** und Antivirenpakete installieren und betreiben zu können, brauchen Sie aber kein lokales Netzwerk einzurichten. Die Rechner müssen lediglich über eine Internetverbindung verfügen.

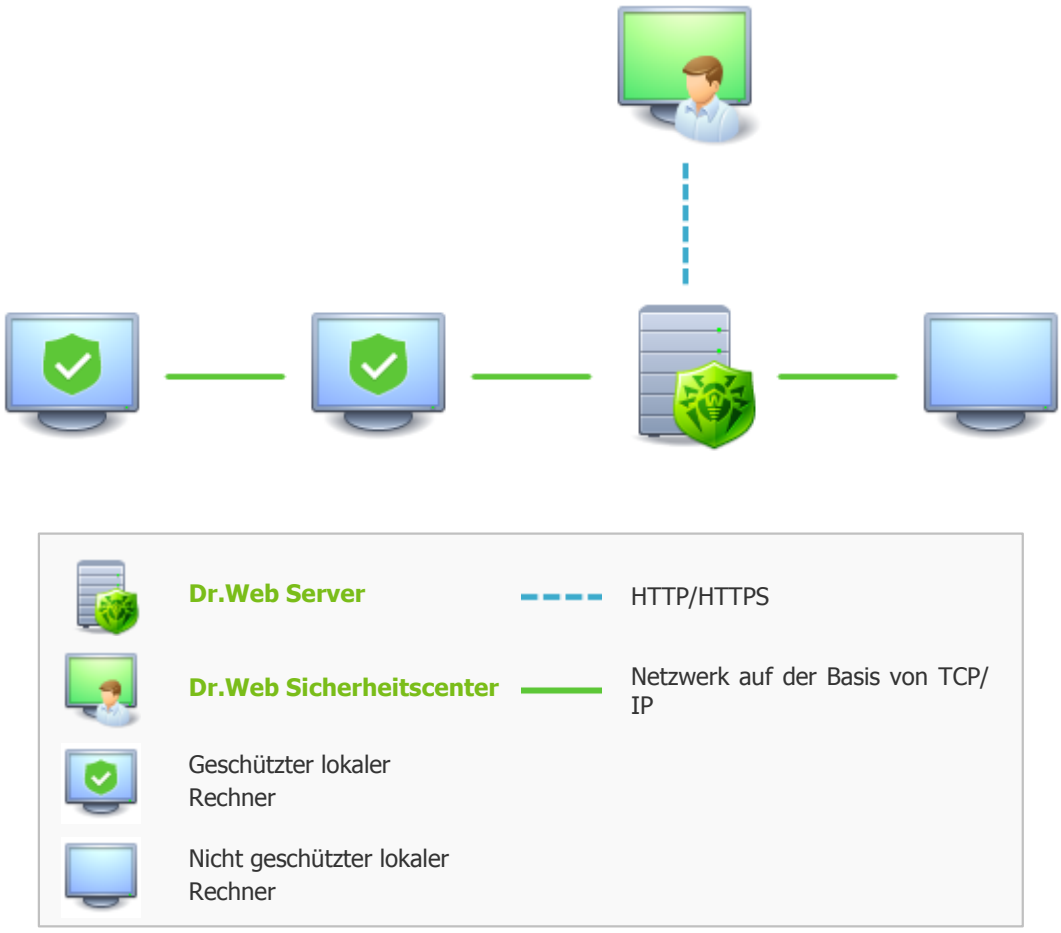


Abbildung2-2: Struktur des Antivirus-Netzwerks

Beim Start des Dr.Web Servers werden die folgenden Aktionen ausgeführt:

1. Herunterladen der Dateien des **Dr.Web Servers** aus dem Verzeichnis `bin`.
2. Herunterladen des **Aufgabenplaners** des **Servers**.
3. Herunterladen der Verzeichnisse für die zentralisierte Installation und Updates; Initialisierung des Benachrichtigungssystems.
4. Überprüfung der Integrität der Datenbank des **Servers**.
5. Ausführung von Aufgaben des **Aufgabenplaners** vom **Server**.
6. Warten auf Informationen von **Dr.Web Agents** und Befehle vom **Verwaltungscenter**.

Alle Befehle, Daten und Statistiken innerhalb des Antivirus-Netzwerks werden zwangsläufig durch den **Dr.Web Server** verarbeitet. Das **Verwaltungscenter** tauscht Informationen nur mit dem **Server** aus. Alle Änderungen in der Konfiguration der Workstation sowie die Befehlsübermittlung an den **Dr.Web Agent** erfolgen durch den **Server** auf der Basis von Befehlen des **Verwaltungscenters**.

Die logische Struktur eines Fragments vom Antivirus-Netzwerk sieht also so aus, wie es in der Abbildung 2-3 dargestellt ist.

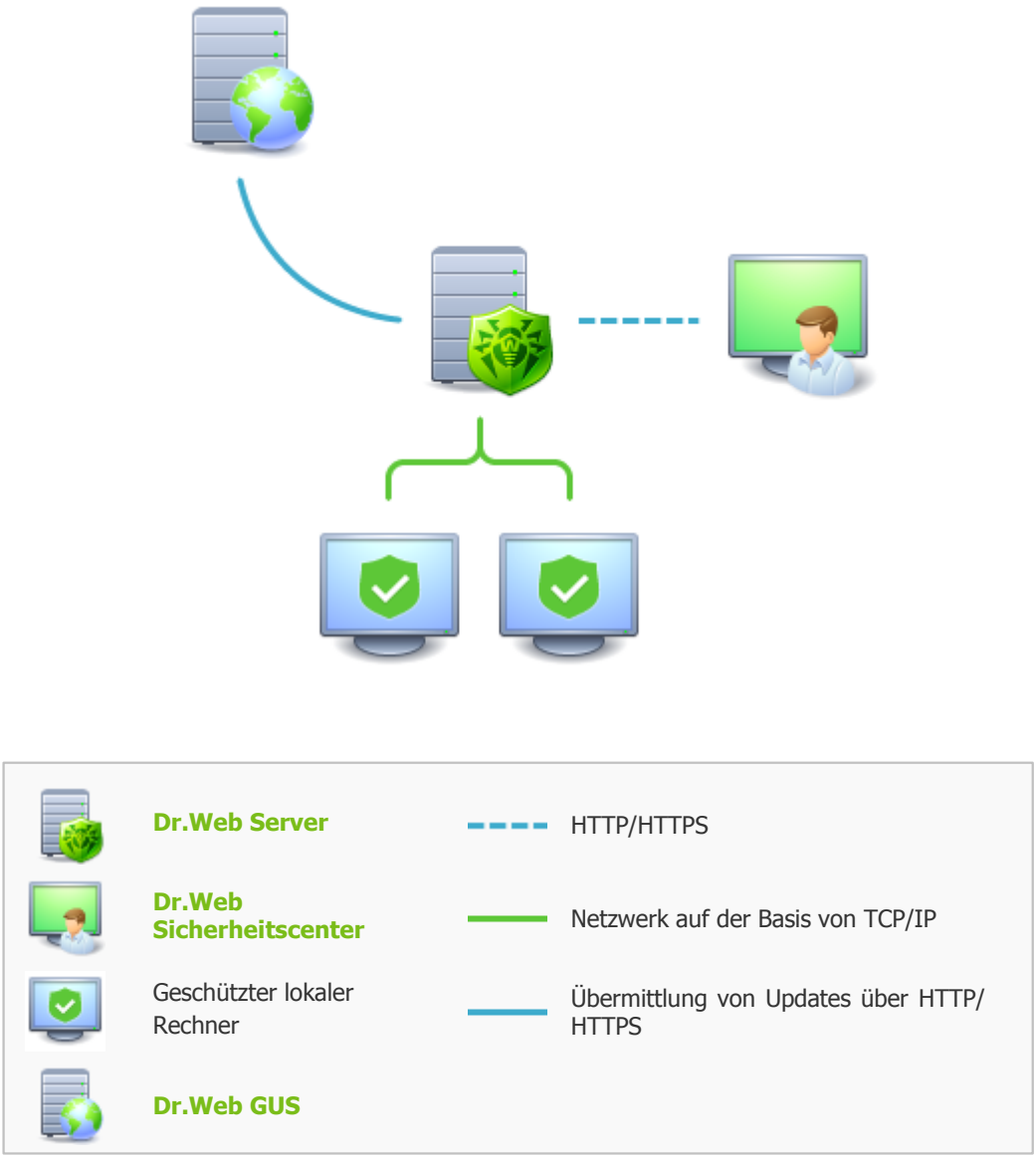


Abbildung 2-3: Logische Struktur des Antivirus-Netzwerks

Zwischen dem **Server** und Workstations (dünne fortlaufende Linie in der Abbildung 2-3) werden die folgenden Informationen ausgetauscht:

- Anforderungen des **Agents** auf den zentralisierten Zeitplan sowie zentralisierten Zeitplan einer bestimmten Workstation.
- Einstellungen des **Agents** und Antivirenpakets.
- Anforderungen auf anstehende Aufgaben (Scannen, Aktualisierung von Virendatenbanken usw.).
- Dateien der Antivirenpakete, wenn der **Agent** die Aufgabe erhält, sie zu installieren.

- Updates für die Software und Virendatenbanken, wenn die Aufgabe zur Aktualisierung ausgeführt wird.
- Nachrichten des **Agents** über die Konfiguration der Workstation.
- Statistiken zum **Agent** und zu den Antivirenpaketen, die in das Gesamtprotokoll aufgenommen werden sollen.
- Nachrichten über erkannte Bedrohungen und andere zu protokollierende Ereignisse.

Das Volumen des Datenverkehrs zwischen Workstations und dem **Server** variiert je nach Einstellungen auf Workstations und kann unter Umständen ziemlich groß sein. Aus diesem Grund ist für **Dr.Web Enterprise Security Suite** die Möglichkeit vorgesehen, den Datenverkehr zu komprimieren. Die Beschreibung dieses optionalen Modus finden Sie unter Datenverkehr verschlüsseln und komprimieren.

Der Datenverkehr zwischen dem **Server** und Workstations kann verschlüsselt werden. Dadurch vermeiden Sie die Offenlegung der Informationen, die über den beschriebenen Kanal übermittelt werden, sowie die Unterschiebung der zu installierenden Software. Diese Option ist standardmäßig aktiviert. Die Beschreibung dieses Modus finden Sie unter Datenverkehr verschlüsseln und komprimieren.

Vom Update-Webserver an den **Dr.Web Server** (dicke fortlaufende Linie in der Abbildung 2-3) werden über das HTTP-Protokoll die Dateien, die zur Replikation der Verzeichnisse für die zentralisierte Installation und Aktualisierung erforderlich sind, sowie Dienstinformationen über den Ablauf dieses Prozesses übertragen. Die Integrität der übertragenen Informationen (Dateien der Software von **Dr.Web Enterprise Security Suite** und der Antivirenpakete) wird durch die Verwendung der Prüfsummen gewährleistet: Eine bei der Übermittlung beschädigte bzw. untergeschobene Datei wird vom **Server** nicht akzeptiert.

Zwischen dem **Server** und dem **Verwaltungscenter** (gestrichelte Linie in der Abbildung 2-3) werden die Informationen zur Konfiguration des **Servers** (darunter auch Informationen zur Netzwerktopologie) und die Einstellungen von Workstations ausgetauscht. Diese Informationen werden im **Verwaltungscenter** visualisiert. Bei jeder Änderung der Einstellungen durch den Benutzer (den Administrator des Antivirus-Netzwerks) werden die Informationen über die jeweils vorgenommenen Änderungen an den **Server** übertragen.

Die Kommunikation zwischen dem **Verwaltungscenter** und dem ausgewählten **Server** ist erst nach der erfolgreichen Authentifizierung vom Administrator des Antivirus-Netzwerks möglich. Der Administrator muss dafür seinen Anmeldenamen und sein Passwort auf diesem **Server** angeben.

Kapitel 3: Erste Schritte. Allgemeine Informationen

3.1. Einfaches Antivirus-Netzwerk erstellen

Bevor Sie die Antivirensoftware nutzen, ändern Sie, wenn möglich, den Speicherort für die kritischen Daten des **Servers** (mehr dazu finden Sie unter Zeitplan des Dr.Web Servers konfigurieren). Der Sicherungsordner sollte auf einem anderen lokalen Laufwerk angelegt werden, damit Dateien der **Server**-Software und Sicherungskopien nicht gleichzeitig verloren gehen.

Verbindung über das Dr.Web Sicherheitscenter herstellen

Standardmäßig wird der **Dr.Web Server** automatisch nach der Installation sowie bei jedem Neustart des Betriebssystems gestartet (s. auch Dr.Web Server).

Um den **Server** und die Antivirensoftware auf Workstations konfigurieren zu können, müssen Sie eine Verbindung mit dem **Server** über das **Dr.Web Sicherheitscenter** herstellen.

Auf jedem Rechner mit dem Netzwerkzugriff auf den **Dr.Web Server** ist das **Verwaltungscenter** unter der folgenden Adresse verfügbar:

`http://`<*Serveradresse*>`:9080`

oder

`https://`<*Serveradresse*>`:9081`

Geben Sie als <*Serveradresse*> die IP-Adresse oder den Domänennamen des Rechners an, auf dem der **Dr.Web Server** installiert ist.

Geben Sie im Dialogfeld für die Autorisierung den Namen und das Passwort des Administrators an (Standardname des Administrators ist **admin**, als Passwort muss das Passwort eingegeben werden, das Sie bei der Installation des **Servers** festgelegt haben. Mehr dazu finden Sie in der **Installationsanleitung** unter Dr.Web Server installieren).

Sobald eine Verbindung mit dem **Server** hergestellt wurde, öffnet sich das Hauptfenster des **Verwaltungscenters**. In diesem Fenster werden Informationen zum Antivirus-Netzwerk, das von diesem **Server** verwaltet wird, angezeigt (mehr dazu finden Sie unter Dr.Web Sicherheitscenter).

Antivirus-Netzwerk verwalten

Über das **Verwaltungscenter** können Sie den **Server** und das Antivirus-Netzwerk verwalten:

- Workstations erstellen (mehr dazu finden Sie in der **Installationsanleitung** unter Dr.Web Agent installieren);
- Workstations bestätigen;
- Workstations bearbeiten, konfigurieren und entfernen (mehr dazu finden Sie unter Kapitel 6: Workstations verwalten);
- Verbindungen mit benachbarten **Dr.Web Servern** konfigurieren und bearbeiten (mehr dazu finden Sie unter Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern);
- Ereignisprotokolle dieses **Servers** und der benachbarten **Server** sowie andere Daten einsehen.

Die wichtigsten Verwaltungstools befinden sich im Hauptmenü, Verwaltungsmenü und auf der Symbolleiste (mehr dazu finden Sie unter Dr.Web Sicherheitscenter).

Verbindung mit Dr.Web Agent herstellen

Nachdem der **Agent** auf der Workstation mithilfe des Installationspakets (mehr dazu finden Sie in der **Installationsanleitung** unter Installationsdateien) installiert wurde, versucht der **Agent**, eine Verbindung mit dem **Dr.Web Server** herzustellen.

Bei den Standardeinstellungen des **Dr.Web Servers** muss der Administrator die neuen Workstations manuell bestätigen, um sie auf dem **Server** zu registrieren (mehr zur Richtlinie für die Genehmigung neuer Workstations finden Sie unter Verbindungsrichtlinie für Workstations). Die neuen Workstations werden dabei nicht automatisch verbunden, sondern durch den **Server** zur Anfänger-Gruppe hinzugefügt (s. dazu den Abschnitt Systemgruppen und benutzerdefinierte Gruppen).

Antivirensoftware installieren

Die Installation von Komponenten des Antivirenpakets auf der Workstation erfordert dann keine weiteren Eingriffe durch den Administrator.

Auf der Workstations werden die Komponenten des Antivirenpakets installiert, die in den Einstellungen der primären Gruppe der Workstation (mehr dazu finden Sie unter Auswahl der zu installierenden Komponenten des Antivirenpakets) festgelegt wurden.

Die Installation einiger Komponenten der Workstation erfordert möglicherweise einen Neustart des Rechners. Wenn das der Fall ist, erscheint über dem Symbol des **Dr.Web Agents** auf der **Symbolleiste** das gelbe Dreieck mit schwarzem Ausrufezeichen (s. auch den Punkt Dr.Web Agent).

3.2. Netzwerkverbindungen konfigurieren

Allgemeine Informationen

Mit dem **Dr.Web Server** verbinden sich folgende Clients:

- **Dr.Web Agents**
- **Netzwerk-Installer von Dr.Web Agents**
- Andere **Dr.Web Server**

Verbindungen werden immer von Clients initiiert.

Clients und der **Server** können miteinander über die folgenden Wege verbunden werden:

1. Über Direktverbindungen.

   Dieses Verfahren hat mehrere Vorteile, ist aber nicht immer explizit empfehlenswert. In einigen Fällen müssen Sie auf dieses Verbindungsschema verzichten.

2. Mithilfe des Server-Suchdienstes.

   Wenn anders nicht festgelegt, verwenden Clients standardmäßig diesen **Dienst**.

   Dieses Verfahren sollte dann verwendet werden, wenn das ganze System neu konfiguriert werden muss. Das kann der Fall sein, wenn Sie den **Dr.Web Server** auf einen anderen Rechner verschieben bzw. die IP-Adresse des Rechners, auf dem der **Server** installiert ist, ändern möchten.

3. Über SRV-Einträge.

   Mit diesem Verfahren können Sie den **Server** nach dem Namen des Rechners und/oder des **Server**-Dienstes anhand der SRV-Einträge auf dem DNS-Server suchen.

Wenn das Antivirus-Netzwerk von **Dr.Web Enterprise Security Suite** für die Verwendung direkter Verbindungen eingestellt wurde, kann der **Server-Suchdienst** deaktiviert werden. Lassen Sie dafür in den Transporteinstellungen **(Administrierung → Dr.Web Server-Konfiguration→** Registerkarte **Transport**) das Feld **Multicast-Gruppe** leer.

Firewall konfigurieren

Damit die Komponenten des Antivirus-Netzwerks miteinander kommunizieren können, müssen alle verwendeten Ports und Schnittstellen auf allen Rechnern, die zum Antivirus-Netzwerk gehören, geöffnet werden.

Bei der Installation des **Servers** durch das Installationsprogramm können Ausnahmen in der Windows-Firewall automatisch hinzugefügt. Aktivieren Sie dafür das Kontrollkästchen **Serverports und -schnittstellen den Firewall Ausnahmen hinzufügen**.

Bei der Verwendung einer Nicht-Windows-Firewall muss der Administrator des Antivirus-Netzwerks diese Firewall manuell entsprechend konfigurieren.

3.2.1. Direktverbindungen

Dr.Web Server konfigurieren

In den Einstellungen des **Servers** müssen Sie die Adresse angeben (mehr dazu finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen), die zum Empfangen eingehender TCP-Verbindungen abgehört werden soll.

Dieser Parameter wird in den Einstellungen des **Servers** unter **Administrierung → Dr.Web Server-Konfiguration** → Registerkarte **Transport** → im Feld **Adresse** festgelegt.

Standardmäßig lauscht der **Server** an den folgenden Adressen und Ports:

- **Adresse**: Nullwert – „alle Netzwerkschnittstellen" für den Rechner verwenden, auf dem der **Server** installiert ist.
- **Port**: `2193` – den Port `2193` verwenden, der für **Dr.Web Enterprise Security Suite** bei IANA registriert ist.

Bitte beachten Sie: In den Versionen des **Servers 4.XX** wurde der Port `2371` verwendet. In der Version **10.0** wird dieser Port nicht mehr unterstützt.

Damit das ganze System von **Dr.Web Enterprise Security Suite** ordnungsgemäß funktionieren kann, reicht es aus, dass der **Server** mindestens an einem TCP-Port lauscht, der allen Clients bekannt ist.

Dr.Web Agent konfigurieren

Bei der Installation des **Agents** kann die Adresse des **Servers** (IP-Adresse bzw. DNS-Name des Rechners, auf dem der **Dr.Web Server** gestartet wurde) in den Installationseinstellungen explizit angegeben werden:

`drwinst` *<Serveradresse>*

Bei der Installation des **Agents** ist es empfehlenswert, den **Server**-Namen zu verwenden, der bereits beim DNS-Dienst registriert wurde. Dadurch wird das Konfigurieren des Antivirus-Netzwerks vereinfacht, das bei der erneuten Installation vom **Dr.Web Server** auf einem anderen Rechner unvermeidlich ist.

Standardmäßig wird durch den Befehl `drwinst`, der ohne Angabe der Parameter ausgeführt wird, das Netzwerk nach **Dr.Web Servern** gescannt. Dabei wird es versucht, den **Agent** vom ersten im Netzwerk gefundenen **Server** (es handelt sich dabei um den *Multicasting*-Modus, bei dem auch der Server-Suchdienst verwendet wird) zu installieren.

Somit wird die Adresse des **Dr.Web Servers** dem **Agent** bei der Installation bekannt.

Nachträglich können Sie die Adresse des **Servers** in den Einstellungen des **Agents** manuell ändern.

3.2.2. Dr.Web Server-Suchdienst

Bei diesem Verbindungsschema ist die Adresse des **Servers** den Clients vorläufig nicht bekannt. Vor jeder Verbindung wird im Netzwerk nach dem **Server** gesucht. Der Client sendet dabei eine Broadcast-Anfrage an das Netzwerk und wartet auf eine Nachricht des **Servers**, die seine Adresse enthalten soll. Sobald die erforderliche Rückantwort empfanden wird, stellt der Client eine Verbindung mit dem **Server** her.

Dafür muss der **Server** auf ähnliche Anfragen lauschen können.

Dieses Verbindungsschema kann auf mehrere Weisen eingestellt werden. Das Wichtigste dabei ist, dass die für die Clients festgelegte Methode zur Suche nach dem **Server** auf die Einstellungen des **Server**-Antwortteils abgestimmt wird.

In **Dr.Web Enterprise Security Suite** wird standardmäßig den Modus *Multicast over UDP* verwendet:

1. Der **Server** wird in der Multicast-Gruppe registriert, die in den Einstellungen des **Servers** festgelegt wurde.
2. Bei der Suche nach dem **Server** senden die **Agents** Multicast-Anfragen an die Gruppe-Adresse, die unter dem Punkt 1 festgelegt wurde.

Standardmäßig werden die folgenden Werte zum Lauschen durch den **Server** festgelegt (wie bei direkten Verbindungen):

- `udp/231.0.0.1:2193`

Bitte beachten Sie: In den Versionen des **Servers 4.XX** wurde der Port `2371` verwendet. In der Version **10.0** wird dieser Port nicht mehr unterstützt.

Dieser Parameter wird in den Einstellungen des **Servers** unter **Administrierung** → **Dr.Web Server-Konfiguration** → Registerkarte **Transport** → im Feld **Multicast-Gruppe** festgelegt.

3.2.3. Über SRV-Einträge

Clients unter Windows unterstützen *SRV*-Ressourceneinträge (die Formatbeschreibung finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen).

Der **Server** kann mittels SRV-Einträgen wie folgt angesprochen werden:

1. Bei der Installation des **Servers** wird die Registrierung in der Active Directory-Domäne eingestellt. Der entsprechende SRV-Eintrag auf dem DNS-Server wird durch das Installationsprogramm angelegt.

SRV-Einträge auf dem DNS-Server werden entsprechend RFC2782 angelegt (s. http://tools.ietf.org/html/rfc2782).

2. Wenn die Verbindung mit dem **Server** angefordert wird, gibt der Benutzer an, dass diese Verbindung mittels `srv`-Ressourceneinträgen hergestellt werden muss.

   Der Start des Installationsprogramms des **Agents** mit expliziter Angabe des **Servers** sieht beispielsweise wie folgt aus:

   ```
   drwinst srv/drwcs
   ```

3. Der Client verwendet transparent die Funktionen der SRV-Ressourceneinträge, um den **Server** anzusprechen.

Wenn kein **Server** explizit angegeben wird, wird standardmäßig `drwcs` als Name des Services verwendet.

Kapitel 4: Administratoren des Antivirus-Netzwerks

Das Antivirus-Netzwerk muss von vertrauenswürdigen und qualifizierten Mitarbeitern verwaltet werden, die ausreichende Erfahrung im praktischen Umgang mit Netzwerktechnologien sowie sichere Kenntnisse im Bereich von IT-Sicherheit und Virenschutz besitzen. Diese Mitarbeiter müssen über den Vollzugriff auf die Installationsverzeichnisse des **Dr.Web Servers** verfügen. Je nach IT-Sicherheitsrichtlinie des Unternehmens und Personalsituation sollte als Administrator des Antivirus-Netzwerks ein Netzwerkadministrator oder ein Mitarbeiter, der mit ihm eng zusammenarbeitet, eingesetzt werden.

Um das Antivirus-Netzwerk zu verwalten, braucht dessen Administrator keine administrativen Rechte auf den Rechnern, die diesem Antivirus-Netzwerk angehören. Die Remote-Installation eines **Agents** kann aber nur innerhalb eines lokalen Netzwerks durchgeführt werden und erfordert Administratorrechte in diesem Netzwerk. Um den **Dr.Web Server** konfigurieren zu können, braucht der Administrator auch Vollzugriff auf sein Installationsverzeichnis.

4.1. Administratorauthentifizierung

Die Administratorauthentifizierung zur Verbindung mit dem Dr.Web Server kann auf eine der folgenden Weisen erfolgen:

1. Anhand der in der Datenbank des **Servers** gespeicherten Informationen zu Administratoren.
2. Über Active Directory (nur für **Server**-Versionen unter Windows).
3. Mittels LDAP-Protokoll.
4. Mittels RADIUS-Protokoll.
5. Über PAM (nur für UNIX-basierte Betriebssysteme)

Die zu verwendende Authentifizierungsmethode wird anhand der folgenden Regeln ausgewählt:

1. Die Auswahl einer Authentifizierungsmethode hängt jeweils von der Reihenfolge der Authentifizierungsmethoden in den Einstellungen ab, die über das **Verwaltungscenter** festgelegt werden.
2. Die Authentifizierung des Administrators anhand der in der Datenbank des **Servers** gespeicherten Anmeldeinformationen hat Vorrang von den anderen Methoden.
3. Wenn diese Informationen fehlen, werden alle anderen Authentifizierungsmethoden standardmäßig in der folgenden Reihenfolge ausprobiert: mittels LDAP-Protokoll, über Active Directory, mittels RADIUS-Protokoll.
4. Zwar kann die Reihenfolge der drei oben genannten Authentifizierungsmethoden in den Einstellungen des **Servers** geändert werden, doch hat die Authentifizierung mithilfe der Anmeldeinformationen in der Datenbank den höchsten Vorrang.
5. Standardmäßig ist die Authentifizierung mittels LDAP- bzw. RADIUS-Protokoll und über Active Directory deaktiviert.

So ändern Sie die Reihenfolge der Authentifizierungsmethoden

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Verwaltungsmenü den Punkt **Authentifizierung**.
3. Im geöffneten Fenster finden Sie die Liste der verfügbaren Authentifizierungsmethoden in der Reihenfolge, in der sie momentan verwendet werden. Die Reihenfolge der Authentifizierungsmethoden lässt sich einfach per Drag-and-drop in der gewünschten Reihenfolge anordnen.
4. Damit die vorgenommenen Änderungen wirksam werden, starten Sie den **Server** neu.

Der Anmeldename des Administrators muss eindeutig sein.

Administratoren können sich mit dem **Server** über externe Authentifizierungssysteme nicht verbinden, wenn ein Administrator mit dem gleichen Anmeldenamen bereits vorhanden ist.

4.1.1. Administratorauthentifizierung mithilfe der Anmeldeinformationen in der Datenbank des Servers

Die Authentifizierung mithilfe der in der Datenbank des **Servers** gespeicherten Informationen zu Administratoren wird standardmäßig verwendet.

So verwalten Sie die Liste der Administratoren

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Verwaltungsmenü den Punkt **Administratoren**. Es öffnet sich die Liste mit allen Administratoren des **Servers**.

Mehr dazu finden Sie unter Administratoren und administrative Gruppen.

4.1.2. Authentifizierung über Active Directory

So aktivieren Sie die Authentifizierung über Active Directory

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Verwaltungsmenü den Punkt **Authentifizierung**.
3. Wechseln Sie im geöffneten Fenster zum Bereich **Microsoft Active Directory**.
4. Aktivieren Sie das Kontrollkästchen **Microsoft Active Directory Autorisierung verwenden**.
5. Klicken Sie auf **Speichern**.
6. Damit die vorgenommenen Änderungen wirksam werden, starten Sie den **Server** neu.

Bei der Authentifizierung über Active Directory wird im **Verwaltungscenter** nur die Berechtigung zum Verwenden dieser Authentifizierungsmethode festgelegt.

Die Eigenschaften der Administratoren von Active Directory werden manuell auf dem Server von Active Directory bearbeitet.

So bearbeiten Sie Administratoren von Active Directory

Die folgenden Aktionen müssen auf den Rechnern vorgenommen werden, auf denen das Active Directory-Snap-In vorhanden ist.

1. Um die Parameter der Administratoren bearbeiten zu können, müssen Sie die folgenden Aktionen durchführen:
   a) Starten Sie zur Änderung des Active Directory-Schemas das Dienstprogramm `drweb-esuite-modify-ad-schema-xxxxxxxxxxxxxx-windows-nt-xYY.exe` (dieses ist in der Distribution des **Dr.Web Servers** enthalten).
   Der Vorgang kann einige Zeit dauern. Je nach Konfiguration Ihrer Domäne kann es mehr als 5 Minuten dauern, bis das geänderte Schema synchronisiert und übernommen wird.

Wenn Sie das Active Directory-Schema mithilfe des Dienstprogramms der **Server**-Version **6** bereits geändert haben, brauchen Sie es mithilfe des Dienstprogramms der **Server**-Version **10.0** nun nicht erneut zu ändern.

b) Um das Snap-In für das Active Directory-Schema zu registrieren, führen Sie mit administrativen Rechten den Befehl `regsvr32 schmmgmt.dll` aus, starten Sie danach `mmc` und fügen Sie das Snap-In **Active Directory Schema** hinzu.

c) Fügen Sie mithilfe des hinzugefügten Active Directory-Schema-Snap-Ins zur Klasse **User** und (falls erforderlich) zur Klasse **Group** die Erweiterungsklasse **DrWebEnterpriseUser** hinzu.

Bis das geänderte Schema komplett übernommen wird, kann es vorkommen, dass die Klasse **DrWebEnterpriseUser** nicht gefunden wird. Warten Sie in diesem Fall einige Zeit und versuchen Sie später, die Klasse wie unter **c)** beschrieben erneut hinzuzufügen.

d) Starten Sie mit Administratorrechten die Datei `drweb-esuite-aduac-xxxxxxxxxxxxx-windows-nt-xYY.msi` (ist in der Distribution von **Dr.Web Enterprise Security Suite 10.0** enthalten) und warten Sie, bis der Installationsvorgang abgeschlossen ist.

2. Die grafische Benutzeroberfläche zum Bearbeiten der Attribute ist verfügbar in der Systemsteuerung **Active Directory Users and Computers** → unter **Users** → im Fenster zum Bearbeiten der Einstellungen des ausgewählten Benutzers **Administrator Properties** → auf der Registerkarte **Dr.Web Authentication**.
3. Der folgende Parameter kann bearbeitet werden (mögliche Attributwerte sind **yes**, **no** oder **not set**):
   - **User is administrator** weist darauf hin, dass der Benutzer Administratorrechte hat.

Die Funktionsweise und Auswertung der Attribute bei der Authentifizierung werden im Dokument **Anhänge** im Anhang C1 detailliert beschrieben.

4.1.3. Authentifizierung mittels LDAP-Protokoll

So aktivieren Sie die LDAP-Authentifizierung

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Verwaltungsmenü den Punkt **Authentifizierung**.
3. Wechseln Sie im geöffneten Fenster zum Bereich PAM-Authentifizierung**.**
4. Aktivieren Sie das Kontrollkästchen **PAM-Authentifizierung verwenden**.
5. Klicken Sie auf **Speichern**.
6. Damit die vorgenommenen Änderungen wirksam werden, starten Sie den **Server** neu.

Die Authentifizierung mittels LDAP-Protokoll kann auf einem beliebigen LDAP-Server konfiguriert werden. Sie können diesen Mechanismus dafür verwenden, um den **Server** unter einem der UNIX-artigen Betriebssysteme zur Authentifizierung in Active Directory auf einem Domänencontroller zu konfigurieren.

Einstellungen für die LDAP-Authentifizierung werden in der Konfigurationsdatei `auth-ldap.xml` gespeichert.

Die wichtigsten XML-Attribute werden im Dokument **Anhänge** im Anhang C2 beschrieben.

Im Unterschied zur Authentifizierung über Active Directory kann dieser Mechanismus für ein beliebiges LDAP-Schema konfiguriert werden. Standardmäßig wird versucht, die Attribute von **Dr.Web Enterprise Security Suite** so zu verwenden, wie sie für Active Directory festgelegt sind.

Die LDAP-Authentifizierung erfolgt auf die folgende Weise:

1. Die Adresse des LDAP-Servers wird über das **Verwaltungscenter** oder in der XML-Konfigurationsdatei festgelegt.

2. Für den festgelegten Benutzernamen werden die folgenden Aktionen ausgeführt:
   - Der Name wird in DN (Distinguished Name) mittels DOS-artigen Masken (getrennt durch das Sternchen *) übersetzt, wenn die Regeln festgelegt sind.
   - Der Name wird in DN mittels regulären Ausdrücken übersetzt, wenn die Regeln festgelegt sind.
   - Für die Übersetzung des Namens in DN wird ein benutzerdefiniertes Skript verwendet, wenn dieses Skript in den Einstellungen angegeben ist.
   - Wenn keine der Übersetzungsregeln passt, wird der angegebene Name verwendet.

Das Format des Benutzernamens ist nicht vordefiniert und kann unternehmensspezifisch bestimmt werden. Keine zwangsläufige Modifizierung des LDAP-Schemas ist erforderlich. Dieses Schema wird mittels der Regeln für die Übersetzung der Namen in LDAP DN entsprechend angepasst.

3. Nachdem der Übersetzungsvorgang abgeschlossen ist, wird es (wie bei der Active Directory-Authentifizierung) versucht, diesen Benutzer anhand des erhaltenen DN und eingegebenen Passworts auf dem angegebenen LDAP-Server zu registrieren.
4. Danach werden die Attribute des LDAP-Objekts für den erhaltenen DN gelesen. Die Attribute und ihre möglichen Werte können in der Konfigurationsdatei erneut definiert werden.
5. Falls nicht definierte Werte der Administrator-Attribute gefunden wurden und in der Konfigurationsdatei die Vererbung festgelegt wurde, wird es nach erforderlichen Attributen in Gruppen gesucht, zu denen der Benutzer gehört. Dieser Prozess ist dem ähnlich, der bei der Active Directory-Authentifizierung stattfindet.

4.1.4. Authentifizierung mittels RADIUS-Protokoll

So aktivieren Sie die RADIUS-Authentifizierung

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Verwaltungsmenü den Punkt **Authentifizierung**.
3. Wechseln Sie im geöffneten Fenster zum Bereich RADIUS-Authentifizierung**.**
4. Aktivieren Sie das Kontrollkästchen **RADIUS-Authentifizierung verwenden**.
5. Klicken Sie auf **Speichern**.
6. Damit die vorgenommenen Änderungen wirksam werden, starten Sie den **Server** neu.

Um die RADIUS-Authentifizierung und das RADIUS-Authentifizierungsprotokoll zu verwenden, müssen Sie einen Server einrichten, der dieses Protokoll unterstützen kann. Zum Beispiel, freeradius (mehr dazu finden Sie unter http://freeradius.org/).

Im **Verwaltungscenter** werden die folgenden Einstellungen für die Verbindung mit dem RADIUS-Server konfiguriert:

- **Server**, **Port**, **Passwort** sind für die Verbindung mit dem RADIUS-Server notwendig: IP-Adresse/ DNS-Name, Portnummer, Passwort (Geheimnis).
- **Timeout** ist das Zeitlimit (in Sekunden) beim Warten auf die Antwort vom RADIUS-Server.
- **Anzahl der Wiederholungsversuche** ist die Anzahl der Versuche, eine Verbindung mit dem RADIUS-Server herzustellen.

Zum Konfigurieren zusätzlicher RADIUS-Einstellungen stehen auch die folgenden Möglichkeiten zur Verfügung:

- Die Konfigurationsdatei `auth-radius.xml` im Verzeichnis `etc` des **Servers**.

Neben Einstellungen, die über das **Verwaltungscenter** konfiguriert werden, können Sie in der Konfigurationsdatei einen Wert für den NAS-Bezeichner festlegen. Dieser RFC 2865-konforme Bezeichner kann anstatt der IP-Adresse/des DNS-Namens als Clientbezeichner bei der Verbindung mit dem RADIUS-Server verwendet werden. Gespeichert wird in der Konfigurationsdatei in der folgenden Form:

```
<!-- NAS identifier, optional, default - hostname -->
<nas-id value="drwcs"/>
```

- Das Wörterbuch `dictionary.drweb` im Verzeichnis `etc` des **Servers**.

  Dieses Wörterbuch enthält die Liste der RADIUS-Attribute des Unternehmens **Doctor Web** (VSA – Vendor-Specific Attributes).

4.1.5. Authentifizierung über PAM

So aktivieren Sie die PAM-Authentifizierung

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Verwaltungsmenü den Punkt **Authentifizierung**.
3. Wechseln Sie im geöffneten Fenster zum Bereich **PAM-Authentifizierung**.
4. Aktivieren Sie das Kontrollkästchen **PAM-Authentifizierung verwenden**.
5. Klicken Sie auf **Speichern**.
6. Damit die vorgenommenen Änderungen wirksam werden, starten Sie den **Server** neu.

Die PAM-Authentifizierung unter UNIX-basierten Betriebssystemen erfolgt mittels austauschbaren Authentifizierungsmodulen.

Die PAM-Authentifizierung kann auf einem der folgenden Wege konfiguriert werden:

- Durch die Authentifizierungseinstellungen im **Verwaltungscenter**: im Bereich **Administrierung** → **Authentifizierung** → **PAM-Authentifizierung**.
- Anhand der Konfigurationsdatei `auth-pam.xml` im Verzeichnis `etc` des **Servers**. Unten finden Sie das Beispiel einer Konfigurationsdatei:

```
...
<!-- Enable this authorization module -->
 <enabled value="no" />
<!-- This authorization module number in the stack -->
  <order value="50" />
<!-- PAM service name>" -->
  <service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
 <admin-flag mandatory="no" name="DrWeb_ESuite_Admin" />
...
```

Beschreibung der Einstellungen für die PAM-Authentifizierung, die in Dr.Web Enterprise Security Suite festgelegt werden

Element des Verwaltungscenters	Elemente der Datei auth-pam.xml			Erläuterung
	Block	Parameter	Zulässige Werte	
Das Kontrollkästchen **PAM-Authentifizierung verwenden**	`<enabled>`	`value`	yes | no	Das Kontrollkästchen bestimmt, ob die PAM-Authentifizierung verwendet werden soll.

Element des Verwaltungscenters	Elemente der Datei auth-pam.xml			Erläuterung
	Block	Parameter	Zulässige Werte	
Drag-and-Drop verwenden	<order>	value	Positive Ganzzahl, die auf Werte der anderen Methoden abgestimmt sein muss	Die laufende Nummer der PAM-Authentifizierung bei der Verwendung mehrerer Authentifizierungsmethoden.
Das Feld **Dienstname**	<service>	name	-	Der Name des Dienstes, der zur Erstellung des PAM-Kontextes verwendet werden soll. PAM kann die Richtlinien für diesen Dienst aus `/etc/pam.d/<Dienstname>` oder `/etc/pam.conf` entnehmen, sofern die Datei vorhanden ist. Wenn der Parameter nicht festgelegt wurde (kein Tag <service> in der Konfigurationsdatei), wird standardmäßig der Name `drwcs` verwendet.
Das Kontrollkästchen **Steuerkennzeichen ist obligatorisch**	<admin-flag>	mandatory	yes | no	Dieser Parameter gibt an, ob das Steuerkennzeichen für die Administrator-Identifikation des Benutzers erforderlich ist. Der Standardwert ist `yes`.
Das Feld **Name des Steuerkennzeichens**	<admin-flag>	name	-	Die Zeichenfolge, anhand derer das Steuerkennzeichen der PAM-Module gelesen werden soll. Der Standardwert ist `DrWeb_ESuite_Admin`.

Verwenden Sie beim Konfigurieren der PAM-Module die Parameter, die in **Dr.Web Enterprise Security Suite** festgelegt werden. Achten Sie dabei auf die Werte, die bei nicht festgelegten Parametern standardmäßig verwendet werden.

4.2. Administratoren und administrative Gruppen

Um den Bereich zur Verwaltung der administrativen Konten zu öffnen, wählen Sie den Punkt **Administrierung** im Hauptmenü des **Verwaltungscenters**. Wählen Sie im geöffneten Fenster den Punkt des Verwaltungsmenüs **Administratoren**.

Der Bereich **Administratoren** ist für alle Administratoren des **Verwaltungscenters** zugänglich. Die gesamte hierarchische Struktur der Administratoren ist aber nur für die Administratoren der Gruppe **Administrators** verfügbar, denen die Berechtigung **Eigenschaften und Konfiguration von Administrationsgruppen einsehen** vergeben wurde. Für sonstige Administratoren wird in der hierarchischen Struktur nur ihre jeweilige Gruppe und deren Untergruppen mit den zu ihnen gehörigen Konten angezeigt.

Hierarchie der Administratoren

Die hierarchische Liste der Administratoren stellt eine Struktur der administrativen Gruppen und Konten dar. Knoten in dieser Struktur sind administrative Gruppen und die zu ihnen gehörigen Administratoren. Jeder Administrator darf nur einer Gruppe angehören. Der Maximalwert ineinander geschachtelter Gruppen ist unbegrenzt.

Vordefinierte Gruppen

Nach der Installation des **Servers** werden zwei Gruppen automatisch erstellt:

- **Administrators**. Zu dieser Gruppe gehört anfangs nur der Administrator **admin**, der volle Rechte besitzt. Dieser Administrator wird bei der Installation des **Servers** automatisch erstellt (s. unten).
- **Newbies**. Ursprünglich ist diese Gruppe leer. In diese Gruppe werden automatisch die Administratoren verschoben, die sich mittels externen Authentifizierungsmethoden, wie etwa über LDAP, Active Directory und RADIUS, authentifizieren.

  Administratoren der Gruppe **Newbies** verfügen standardmäßig nur über den Lesezugriff.

Vordefinierte Administratoren

Nach der Installation des **Servers** wird automatisch das folgende Konto erstellt:

Parameter	Wert
Anmeldename	**admin**
Passwort	Das Passwort wird bei der Installation des **Servers** angegeben (Schritt 15 im Installationsverfahren).
Rechte	Volle Rechte.
Bearbeitung des Kontos	Die Administratorrechte können nicht bearbeitet werden. Der Administrator kann nicht gelöscht werden.

Anzeige der hierarchischen Listen

- In der hierarchischen Liste des Antivirus-Netzwerks sind für Administratoren nur diejenigen benutzerdefinierten Gruppen sichtbar, die im Recht **Eigenschaften von Stationengruppen einsehen** erlaubt sind. Alle Systemgruppen werden ebenfalls in der Struktur des Antivirus-Netzwerks angezeigt. In diesen Gruppen werden jedoch nur die Workstations aus der angegebenen Liste benutzerdefinierter Gruppen angezeigt.
- In der hierarchischen Liste von Administratoren kann ein Administrator der Gruppe **Newbies** die baumartige Struktur sehen, deren Wurzel die Gruppe ist, in der er sich befindet: Er sieht also Administratoren seiner Gruppe und ihrer Untergruppen. Für einen Administrator der Gruppe **Administrators** sind Administratoren aller Gruppen sichtbar.

Rechte der Administratoren

Alle Aktionen der Administratoren im **Verwaltungscenter** werden anhand eines Berechtigungssatzes geregelt. Dieser kann sowohl für ein bestimmtes Konto als auch für eine administrative Gruppe festgelegt werden.

Durch das System der administrativen Rechte können die folgenden Berechtigungen verwaltet werden:

- **Erteilung der Rechte**

  Rechte werden bei der Erstellung eines Administrators oder einer administrativen Gruppe zugewiesen. Sie werden von der übergeordneten Gruppe geerbt, in die der Administrator oder die administrative Gruppe bei der Erstellung verschoben wird. Rechte können bei der Erstellung nicht geändert werden.

- **Vererbung der Rechte**

  Die Rechte der Administratoren und administrativen Gruppen werden standardmäßig von der übergeordneten Gruppe geerbt. Die Vererbung kann aber deaktiviert werden.

  Einem Konto kann ein beliebiger Berechtigungssatz zugewiesen werden. Alle anderen Berechtigungen werden von der übergeordneten Gruppe geerbt, in der sich der jeweilige Administrator befindet. Bei der Vererbung der Berechtigungen des Administrators oder der Gruppe werden diese nicht erneut zugewiesen. Stattdessen wird ein neuer Berechtigungssatz anhand aller Berechtigungen in den übergeordneten Gruppen der Hierarchie zusammengestellt. Die Tabelle zur Berechnung der resultierenden Berechtigung des Objekts je nach Vererbung und Rechten der übergeordneten Gruppen finden Sie im Dokument **Anhänge** im Anhang C3.

- **Rechte bearbeiten**

  Bei der Erstellung von Administratoren oder administrativen Gruppen können keine Rechte bearbeitet werden. Die Bearbeitung der Rechte ist nur für erstellte Objekte möglich und wird in den Einstellungen des jeweiligen Kontos oder der Gruppe vorgenommen. Bei der Bearbeitung ist nur eine Reduzierung der Rechte möglich. Die Rechte des vordefinierten Administrators **admin** können nicht geändert werden.

  Die Bearbeitung der Rechte wird unter Administrative Konten und Gruppen bearbeiten detailliert beschrieben.

Eine kurze Beschreibung der Rechte von Administratoren und der Bereiche des **Verwaltungscenters**, auf die sie Auswirkungen haben, finden Sie im Dokument **Anhänge** im Anhang C4.

4.3. Administratorkonten und administrative Gruppen verwalten

4.3.1. Administrative Konten und Gruppen erstellen und löschen

Der Anmeldename des Administrators muss eindeutig sein.

Administratoren können sich mit dem **Server** über externe Authentifizierungssysteme nicht verbinden, wenn ein Administrator mit dem gleichen Anmeldenamen bereits vorhanden ist.

Administratorkonten hinzufügen

Zur Erstellung von Administratorkonten ist die Berechtigung **Administratoren bzw. Administrationsgruppen erstellen** erforderlich.

So erstellen Sie ein Administratorkonto

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Administratoren**.

2. Klicken Sie in der Symbolleiste auf das Symbol **Konto erstellen**. Es öffnet sich das Fenster zum Einstellen des zu erstellenden Kontos.
3. Geben Sie im Unterbereich **Allgemein** die folgenden Parameter an:
   - Geben Sie ins Feld **Anmeldename** den Anmeldename des Administrators ein, der für den Zugriff auf das **Verwaltungscenter** verwendet werden soll. Erlaubt sind Kleinbuchstaben (a-z), Großbuchstaben (A-Z), Zahlen (0-9), Zeichen „_" und „.".
   - Wählen Sie in der Liste **Authentifizierungstyp** eine der folgenden Varianten aus:
     - **Intern**. Der Administrator wird im **Verwaltungscenter** anhand der Anmeldedaten in der Datenbank des **Dr.Web Servers** authentifiziert.
     - **Extern**. Der Administrator wird im **Verwaltungscenter** über externe Systeme, wie etwa über LDAP, Active Directory, RADIUS oder PAM, authentifiziert.

   Mehr dazu finden Sie unter Administratorauthentifizierung.

   - Geben Sie in die Felder **Passwort** und **Passwort bestätigen** ein Passwort für den Zugriff auf den **Server** und das **Verwaltungscenter** ein.

   Bei der Eingabe des Passworts sind keine nationalen Sonderzeichen erlaubt.

   - Optional können Sie in den Feldern **Name**, **Vorname** und **Zwischenname** persönliche Daten des Administrators angeben.
   - Wählen Sie in der Dropdown-Liste die **Sprache der Benutzeroberfläche** des **Verwaltungscenters** aus. Diese wird vom zu erstellenden Administrator verwendet (standardmäßig wird die Sprache des Webbrowsers bzw. Englisch verwendet).
   - Wählen Sie in der Dropdown-Liste **Datumsformat** das Format, das von diesem Administrator beim Bearbeiten der Einstellungen, die ein Datum enthalten, verwendet wird. Zur Verfügung stehen die folgenden Formate:
     - `DD-MM-YYYY HH:MM:SS`
     - `MM/DD/YYYY HH:MM:SS`
   - Geben Sie ins Feld **Beschreibung** eine kurze Beschreibung des Kontos ein (optional).

   Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

4. Im Unterbereich **Gruppen** wird eine übergeordnete administrative Gruppe festgelegt. Die Liste enthält die Gruppen, denen ein Administrator zugewiesen werden kann. Neben der Gruppe, welcher der zu erstellende Administrator zugewiesen werden soll, wird ein Häkchen gesetzt. Standardmäßig gehören alle neu erstellten Administratoren zur übergeordneten Gruppe des aktuellen Administrators. Um eine andere Gruppe auszuwählen, setzen Sie ein Häkchen neben der gewünschten Gruppe.

   Jeder Administrator kann nur einer Gruppe angehören.

   Der Administrator vererbt die Rechte der übergeordneten Gruppe (mehr dazu finden Sie unter Rechte der Administratoren).

5. Nachdem alle erforderlichen Parameter festgelegt sind, klicken Sie auf **Speichern**, um ein neues Administratorkonto zu erstellen.

Administrative Gruppen hinzufügen

Zur Erstellung von administrativen Gruppen ist die Berechtigung **Administratoren bzw. Administrationsgruppen erstellen** erforderlich.

So fügen Sie eine neue administrative Gruppe hinzu

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Administratoren**.
2. Klicken Sie in der Symbolleiste auf das Symbol **Gruppe erstellen**. Es öffnet sich das Fenster zum Einstellen der zu erstellenden Gruppe.
3. Geben Sie im Unterbereich **Allgemein** die folgenden Parameter an:
   - Geben Sie ins Feld **Gruppe** einen Namen für die zu erstellende administrative Gruppe ein. Erlaubt sind Kleinbuchstaben (a-z), Großbuchstaben (A-Z), Zahlen (0-9), Zeichen „_" und „.".
   - Geben Sie ins Feld **Beschreibung** eine kurze Beschreibung der Gruppe ein (optional).
4. Im Unterbereich **Gruppen** wird eine übergeordnete administrative Gruppe festgelegt. Die Liste enthält die Gruppen, die als übergeordnete Gruppen verwendet werden können. Neben der Gruppe, in welche die zu erstellende Gruppe aufgenommen werden soll, wird ein Häkchen gesetzt. Standardmäßig gehören alle neu erstellten Gruppen zur übergeordneten Gruppe des aktuellen Administrators. Um eine andere Gruppe auszuwählen, setzen Sie ein Häkchen neben der gewünschten Gruppe.

   Nur eine übergeordnete Gruppe kann zugewiesen werden.

   Die erstellte administrative Gruppe vererbt die Rechte der übergeordneten Gruppe (mehr dazu finden Sie unter Rechte der Administratoren).
5. Nachdem alle erforderlichen Parameter festgelegt sind, klicken Sie auf **Speichern**, um eine neue administrative Gruppe zu erstellen.

Administratorkonten und administrative Gruppen löschen

Um Administratorkonten und administrative Gruppen löschen zu können, müssen Sie über die Rechte **Administratorkonten löschen** und **Eigenschaften und Konfiguration von Administrationsgruppen bearbeiten** verfügen.

So löschen Sie ein Administratorkonto oder eine Gruppe

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Administratoren**.
2. Wählen Sie in der hierarchischen Liste der Administratoren das Administratorkonto bzw. die administrative Gruppe, die Sie löschen wollen.
3. Klicken Sie auf der Symbolleiste auf **Ausgewählte Objekte entfernen**.

4.3.2. Administrative Konten und Gruppen bearbeiten

Um Administratorkonten und administrative Gruppe bearbeiten zu können, müssen Sie über die Rechte **Administratorkonten bearbeiten** und **Eigenschaften und Konfiguration von Administrationsgruppen bearbeiten** verfügen.

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

Administratorkonten bearbeiten

So bearbeiten Sie ein Administratorkonto

1. Wählen Sie in der Liste der Administratoren das Administratorkonto, das Sie bearbeiten wollen. Beim Klicken auf den Namen des Kontos öffnet sich der Bereich zum Bearbeiten der Eigenschaften.
2. In der Unterbereich **Allgemein** können Sie die Parameter bearbeiten, die bei der Erstellung festgelegt wurden.

   a) Um das Passwort für den Zugriff auf das Administratorkonto zu ändern, wählen Sie in der Symbolleiste das Symbol **Passwort ändern**.

   Der Administrator mit den entsprechenden Rechten kann die Passwörter aller anderen Administratoren ändern.

   Bei der Angabe des Anmeldenamens sind keine nationalen Sonderzeichen erlaubt.

   b) Die folgenden Parameter des Administrators sind schreibgeschützt:

   - Erstellungsdatum des Kontos sowie das Datum der letzten Änderung seiner Einstellungen.
   - **Status**. Er zeigt die Netzwerkadresse der letzten Verbindung unter diesem Konto an.
3. Im Unterbereich **Gruppen** können Sie eine andere administrative Gruppe auswählen. Die Liste enthält die Gruppen, denen ein Administrator zugewiesen werden kann. Die aktuelle übergeordnete Gruppe des Administrators wird durch ein Häkchen gekennzeichnet. Um eine andere Gruppe auszuwählen, setzen Sie ein Häkchen neben der gewünschten Gruppe.

   Jedem Administrator muss unbedingt eine übergeordnete Gruppe zugewiesen werden. Jeder Administrator kann nur einer Gruppe angehören. Die Rechte werden von der zugewiesenen übergeordneten Gruppe geerbt.

   Mehr dazu finden Sie unter Mitgliedschaft bearbeiten.
4. In der Untergruppe **Rechte** können Sie die Liste der Aktionen bearbeiten, die dieser Administrator durchführen darf.

   Die Vorgehensweise bei der Bearbeitung der Rechte wird unter Rechte bearbeiten beschrieben.
5. Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**.

Administrative Gruppen bearbeiten

So bearbeiten Sie eine administrative Gruppe

1. Wählen Sie in der Liste der Administratoren die Gruppe, die Sie bearbeiten wollen. Beim Klicken auf den Namen der Gruppe öffnet sich der Bereich zum Bearbeiten der Eigenschaften.
2. In der Unterbereich **Allgemein** können Sie die Parameter bearbeiten, die bei der Erstellung festgelegt wurden.
3. Im Unterbereich **Gruppen** können Sie eine andere übergeordnete Gruppe auswählen. Die Liste enthält die Gruppen, die als übergeordnete Gruppen verwendet werden können. Die aktuelle übergeordnete Gruppe wird durch ein Häkchen gekennzeichnet. Um eine andere Gruppe auszuwählen, setzen Sie ein Häkchen neben der gewünschten Gruppe.

   Jeder administrativen Gruppe muss unbedingt eine übergeordnete Gruppe zugewiesen werden. Die Rechte werden von der zugewiesenen übergeordneten Gruppe geerbt.

Mehr dazu finden Sie unter Mitgliedschaft bearbeiten.

4. In der Untergruppe **Rechte** können Sie die Liste der erlaubten Aktionen bearbeiten.

   Die Vorgehensweise bei der Bearbeitung der Rechte wird unter Rechte bearbeiten beschrieben.

5. Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**.

Rechte bearbeiten

So ändern Sie die Rechte der Administratoren und administrativen Gruppen im Bereich zum Bearbeiten der Eigenschaften

1. Um die Vererbung zu ändern, klicken Sie in der Überschrift der Rechtetabelle in der Spalte **Vererbung** auf **Aktiviert/deaktiviert** und wählen Sie in der Dropdown-Liste den gewünschten Wert.
2. Die Liste der Rechte wird in drei Unterbereiche aufgeteilt:
   - Rechte zur Verwaltung von Workstations und Gruppen von Workstations.
   - Rechte zur Verwaltung von Administratoren und administrativen Gruppen.
   - Rechte mit Kontrollkästchen.
3. Die Rechte der zwei ersten Unterbereiche werden in den Spalten **Gewährt** und **Verweigert** bearbeitet.

   Die Rechte werden dabei wie folgt verteilt:

Zelleninhalt	Werte in der Spalte	
	Gewährt	**Deaktiviert**
Name der Gruppe oder die Liste von Gruppennamen	Das Recht ist nur für die aufgelisteten Gruppen erlaubt	Das Recht ist nur für die aufgelisteten Gruppen verboten
Alle	Das Recht ist für alle Gruppen erlaubt	Das Recht ist für alle Gruppen verboten
Nichts	Das Recht ist für keine der Gruppen erlaubt	Das Recht ist für keine der Gruppen verboten

Um ein Recht zu bearbeiten, klicken Sie auf den Wert der Zelle mit dem jeweiligen Recht. Es öffnet sich das Fenster zur Auswahl der Gruppen, für die dieses Recht gilt. Wählen Sie in der Liste einen der Werte aus:

Name der Einstellung	Aktion bei der Auswahl der Einstellung
Für Workstations	
Alle	Die Rechteeinstellung wird bei allen Workstations übernommen, die mit diesem **Server** verbunden sind.
Gruppe von Workstations auswählen	Die Rechteeinstellung wird nur bei den Workstations der gewählten Gruppen übernommen. Um bestimmte Gruppen auszuwählen, klicken Sie in der Liste **Antivirus-Netzwerk** auf die gewünschten Gruppen. Eine Mehrfachauswahl gelingt mit gedrückter STRG- oder UMSCHALTTASTE.
Für Administratoren	
Alle	Die Rechteeinstellung wird bei allen Administratoren dieses **Servers** übernommen.
Gruppe von Administratoren auswählen	Die Rechteeinstellung wird nur bei den Administratoren der gewählten administrativen Gruppen übernommen. Um bestimmte Gruppen auszuwählen, klicken Sie in der Liste **Administratoren** auf die gewünschten Gruppen. Eine Mehrfachauswahl gelingt mit gedrückter STRG- oder UMSCHALTTASTE.

4. Zur Verwaltung der Rechte des dritten Unterbereichs aktivieren Sie das Kontrollkästchen neben dem entsprechenden Recht in einer der Spalten **Gewährt** oder **Verweigert**, um dieses Recht für die Administratoren der zu bearbeitenden administrativen Gruppe zu erlauben bzw. zu verbieten.
5. Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**.

Mitgliedschaft bearbeiten

Es gibt mehrere Möglichkeiten, Administratoren und administrativen Gruppen eine übergeordnete Gruppe zuzuweisen.

1. Die Einstellungen des Administrators oder der Gruppe können wie oben beschrieben geändert werden.
2. Alternativ können Sie den Administrator oder die administrative Gruppe in der hierarchischen Liste auf die Gruppe ziehen (per Drag-and-drop), die als die übergeordnete Gruppe verwendet werden soll.

Kapitel 5: Gruppen. Integrierte Verwaltung von Workstations

Mit der Gruppierung lässt sich die Verwaltung von Workstations des Antivirus-Netzwerks erheblich erleichtern.

Die Gruppierung von Workstations bringt die folgenden Vorteile:

- Bestimmte Aktionen können gleichzeitig für alle Workstations der Gruppe durchgeführt werden.

  Sowohl für eine einzelne Gruppe als auch für mehrere ausgewählte Gruppen können Sie Aufgaben zum Scannen von Workstations, die zu dieser Gruppe gehören, starten, einsehen und stoppen. Darüber hinaus können Sie Statistik (z. B. zu Infektionen, Viren, Scan- und Installationsfehlern, zum Starten/Beenden usw.) sowie Gesamtstatistiken für alle Workstations der Gruppe bzw. mehrerer Gruppen einsehen.

- Für alle Workstations einer Gruppe können die gleichen Einstellungen festgelegt werden (mehr dazu finden Sie unter Gruppenbasierte Konfiguration von Workstations).
- Workstations können in der Liste strukturiert angezeigt werden.

Es besteht auch die Möglichkeit, verschachtelte Gruppen zu erstellen.

5.1. Systemgruppen und benutzerdefinierte Gruppen

Systemgruppen

Dr.Web Enterprise Security Suite enthält ursprünglich einen Satz vordefinierter Systemgruppen. Sie werden bei der Installation des **Dr.Web Servers** erstellt und können nicht gelöscht werden. Administratoren können sie aber ausblenden.

Jede Systemgruppe (außer **Everyone**) beinhaltet einen Satz von Untergruppen, die anhand eines bestimmten Merkmals gebildet werden.

Nach der Installation des **Servers**, und bis Workstations mit ihm verbunden werden, wird in der Liste des Systemgruppen nur die Gruppe **Everyone** angezeigt. Um alle Systemgruppen anzeigen zu lassen, verwenden Sie die Option **Ausgeblendete Gruppen anzeigen**, die sich im Bereich **Einstellungen der Verzeichnisstruktur** auf der Symbolleiste befindet.

Everyone

Das ist eine Gruppe, die alle dem **Dr.Web Server** bekannten Workstations beinhaltet. Die Gruppe **Everyone** enthält die Standardeinstellungen aller Gruppen und Workstations.

Configured

Diese Gruppe beinhaltet die Workstations, für die individuelle Einstellungen festgelegt wurden.

Operating system

Diese Kategorie der Untergruppen zeigt die Betriebssysteme, unter denen Workstations momentan laufen. Diese Gruppen sind nicht virtuell und können die Einstellungen der Workstations enthalten sowie als primäre Gruppen auftreten.

- Untergruppen der **Android**-Familie. Diese Familie enthält Gruppen, die einer jeweiligen Version des Android-Betriebssystems für mobile Endgeräte entsprechen.
- Untergruppen der **Mac**-Familie. Diese Familie enthält Gruppen, die einer bestimmten Version des Mac OS X-Betriebssystems entsprechen.
- Untergruppe **Netware**. Diese Untergruppe enthält Workstations unter Novell NetWare.
- Untergruppen der **UNIX**-Familie. Diese Familie enthält Gruppen, die jeweils einem der UNIX-basierten Betriebssysteme entsprechen, z. B. Linux, FreeBSD, Solaris usw.
- Untergruppen der **Windows**-Familie. Diese Familie enthält Gruppen, die jeweils einer bestimmten Version des Windows-Betriebssystems entsprechen.

Status

Die Gruppe **Status** enthält verschachtelte Gruppen, die zur Anzeige des aktuellen Status von Workstations und der Antivirensoftware dienen. Dadurch kann festgestellt werden, ob Workstations momentan mit dem **Server** verbunden sind, oder ob die Antivirensoftware bereits deinstalliert ist bzw. ob ihre Lizenz abgelaufen ist. Diese Gruppen sind komplett virtuell und enthalten keine Einstellungen. Außerdem können sie nicht als primäre Gruppen definiert werden.

- Gruppe **Deinstalled**. Sobald die Antivirensoftware des **Dr.Web Agents** von einer Workstation deinstalliert wurde, wird diese Workstation automatisch in die Gruppe **Deinstalled** verschoben.
- Gruppe **Deleted**. Diese Gruppe enthält Workstations, die durch den Administrator vom **Server** gelöscht wurden. Die gelöschten Workstations können wiederhergestellt werden (mehr dazu finden Sie unter Workstation löschen und wiederherstellen).
- Gruppe **New**. Diese Gruppe enthält die neuen Workstations, die durch den Administrator über das **Verwaltungscenter** zwar erstellt wurden aber noch keinen installierten **Agent** haben.
- Gruppe **Newbies**. Diese Gruppe enthält alle nicht bestätigten Workstations, deren Registrierung auf dem **Server** zum aktuellen Zeitpunkt noch nicht bestätigt wurde. Wird die Registrierung der Workstations bestätigt bzw. wird ihnen Zugriff auf den **Server** verweigert, werden sie aus der Gruppe automatisch entfernt.
- Gruppe **Offline** Diese Gruppe enthält alle Workstations, die mit dem **Server** momentan nicht verbunden sind.
- Gruppe **Online**. Diese Gruppe enthält alle Workstations, die mit dem **Server** momentan verbunden sind (bzw. die seine Anfragen beantworten).
- Gruppe **Update Errors**. Diese Gruppe enthält die Workstations, auf denen die Aktualisierung der Antivirensoftware fehlgeschlagen ist.

Transport

Diese Untergruppen geben das Protokoll an, über das Workstations mit dem **Server** momentan verbunden sind. Diese Untergruppen sind komplett virtuell und enthalten keine Einstellungen. Außerdem können sie nicht als primäre Gruppen definiert werden.

- Gruppe **TCP/IP**. Diese Gruppe enthält die über das TCP/IP-Protokoll Version 4 verbundenen Workstations.
- Gruppe **TCP/IP Version 6**. Diese Gruppe enthält die über das TCP/IP-Protokoll Version 6 verbundenen Workstations.

Ungrouped

Diese Gruppe enthält die Workstations, die keiner der Benutzergruppen angehören.

Benutzerdefinierte Gruppen

Als benutzerdefinierte Gruppen werden die Gruppen bezeichnet, die der Administrator des Antivirus-Netzwerks für eigene Zwecke erstellt. Der Administrator kann eigene Gruppen, verschachtelte Gruppen erstellen und ihnen Workstations hinzufügen. Der Inhalt und Name dieser Gruppen werden durch **Dr.Web Enterprise Security Suite** auf keine Weise begrenzt.

In der Tabelle 5-1 werden alle möglichen Gruppen und Gruppentypen sowie spezifische von diesen Gruppen unterstützte (+) bzw. nicht unterstützte (–) Parameter anschaulich aufgeführt.

Dabei werden die folgenden Parameter berücksichtigt:

- **Automatische Mitgliedschaft**. Dieser Parameter gibt an, ob Workstations der Gruppe automatisch hinzugefügt werden können (automatische Mitgliedschaft), und ob der Inhalt der Gruppe beim Betrieb des **Servers** automatisch geändert werden kann.
- **Mitgliedschaftsverwaltung**. Dieser Parameter gibt an, ob die Mitgliedschaft in einer Gruppe vom Administrator verwaltet werden kann. Es handelt sich dabei um das Hinzufügen bzw. Löschen der Workstations in der Gruppe.
- **Primärgruppe**. Dieser Parameter gibt an, ob diese Gruppe als primäre verwendet werden kann.
- **Eigene Einstellungen**. Dieser Parameter gibt an, ob die Gruppe eigene Einstellungen für Antivirenkomponenten enthalten kann (damit diese von ihren Workstations übernommen werden).

Tabelle 5-1: Gruppen und unterstützte Parameter

Gruppe/Gruppentyp	Parameter			
	Automatische Mitgliedschaft	Mitgliedschaftsverwaltung	Primärgruppe	Eigene Einstellungen
Everyone	+	–	+	+
Configured	+	–	–	–
Operating System	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Ungrouped	+	–	–	–
Benutzerdefinierte Gruppen	–	+	+	+

Unter dem Konto des *Gruppenadministrators* wird die benutzerdefinierte Gruppe, die von diesem Administrator verwaltet wird, in der Wurzel der hierarchischen Baumstruktur angezeigt, selbst wenn diese Gruppe eine übergeordnete Gruppe hat. Alle untergeordneten Gruppen der verwalteten Gruppe sind dabei verfügbar.

5.2. Gruppen verwalten

5.2.1. Gruppen erstellen und löschen

Gruppe erstellen

So erstellen Sie eine neue Gruppe

1. Wählen Sie auf der Symbolleiste den Punkt **Station oder Gruppe hinzufügen** und klicken Sie dann im Untermenü auf **Gruppe erstellen**.

   Es öffnet sich das Fenster, in dem eine neue Gruppe erstellt werden kann.
2. Das Feld **Identifikator** wird automatisch ausgefüllt. Das Feld kann ggf. beim Erstellen bearbeitet werden. Der Identifikator darf keine Leerzeichen enthalten. Der Identifikator der Gruppe kann nachträglich nicht geändert werden.
3. Geben Sie im Feld **Name** den gewünschten Namen der Gruppe an.
4. Wählen Sie im Feld **Verwandte Gruppe** für verschachtelte Gruppen die Gruppe aus, die als übergeordnete Gruppe verwendet werden soll und von der die Konfiguration vererbt wird, falls keine individuellen Einstellungen festgelegt wurden. Bei einer Stammgruppe (hat kein übergeordnetes Element) lassen Sie dieses Feld leer: Die Gruppe wird zur Wurzel der hierarchischen Liste hinzugefügt. In diesem Fall werden die Einstellungen aus der Gruppe **Everyone** übernommen.
5. Geben Sie ins Feld **Beschreibung** einen optionalen Kommentar ein.
6. Klicken Sie auf **Speichern**.

Die von Ihnen erstellten Gruppen sind am Anfang leer. Um Workstations diesen Gruppen hinzuzufügen, gehen Sie so vor wie unter Workstations zu benutzerdefinierten Gruppen hinzufügen beschrieben.

Gruppe löschen

So löschen Sie eine bestehende Gruppe

1. Wählen Sie in der hierarchischen Liste des **Verwaltungscenters** eine benutzerdefinierte Gruppe aus.
2. Klicken Sie auf der Symbolleiste auf **Allgemein** → **Ausgewählte Objekte entfernen**.

> Vordefinierte Gruppen können nicht gelöscht werden.

5.2.2. Gruppen bearbeiten

So ändern Sie die Einstellungen einer Gruppe

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Bereich **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste des geöffneten Fensters eine Gruppe aus.
2. Öffnen Sie auf eine der folgenden Weisen den Bereich der Gruppeneigenschaften:
   a) Klicken Sie auf **Allgemein** → **Editieren** auf der Symbolleiste. Die Eigenschaften der Gruppe werden im rechten Bereich des **Verwaltungscenters** angezeigt.
   b) Wählen Sie den Punkt **Eigenschaften** des Verwaltungsmenüs. Es öffnet sich das Fenster mit den Eigenschaften der Gruppe.
3. Das Fenster der Eigenschaften der Gruppe enthält die Bereiche **Allgemein** und **Konfiguration**. Ihre Einstellungen werden unten beschrieben.

> Bei der Anzeige der Gruppeneigenschaften im rechten Teil des **Verwaltungscenters** (s. den Punkt **2.a)**) ist auch der Bereich **Informationen über die Stationen** verfügbar. In diesem Bereich werden allgemeine Informationen zu den Workstations, die zu dieser Gruppe gehören, angezeigt.

4. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie auf **Speichern**.

Allgemein

Der Bereich **Allgemein** enthält die folgenden Informationen:

- **Identifikator**. Hier ist die eindeutige schreibgeschützte ID der Gruppe angegeben.
- **Name**. Hier ist der Name der Gruppe angegeben. Der Name einer benutzerdefinierten Gruppe kann ggf. geändert werden. Bei vordefinierten Gruppen kann das Feld **Name** nicht bearbeitet werden.
- **Verwandte Gruppe**. Hier ist die übergeordnete Gruppe angegeben, zu der diese Gruppe gehört und von der die Konfiguration geerbt wird, falls keine individuellen Einstellungen festgelegt wurden. Wenn keine übergeordnete Gruppe zugewiesen ist, werden die Einstellungen von der Gruppe **Everyone** geerbt.
- **Beschreibung**. Das ist ein optionales Feld mit der Beschreibung der Gruppe.

Informationen über die Stationen

Der Bereich **Informationen über die Stationen** enthält die folgenden Informationen:

- **Stationen**. Das ist die Gesamtzahl der Workstations, die zu dieser Gruppe gehören.
- **Primärgruppe für**. Das ist die Anzahl der Workstations, für welche diese Gruppe primär ist.
- **Stationen im Netzwerk**. Hier wird die Anzahl der Workstations, die zum aktuellen Zeitpunkt aktiv (online) sind.

Konfiguration

> Informationen zur Vererbung von Gruppeneinstellungen durch die Workstations, für die diese Gruppe primär ist, finden Sie unter Gruppenbasierte Konfiguration von Workstations.

Im Bereich **Konfiguration** können Sie die Konfiguration der Gruppen ändern. Die Konfiguration besteht aus den folgenden Parametern:

Symbol	Einstellungen	Abschnitt mit der Beschreibung
	Rechte der Benutzer von Workstations, die diese Einstellung von der Gruppe vererben, falls diese primär ist. Die Einstellung der Gruppenrechte ist der Einstellung von Rechten einzelner Workstations ähnlich.	Berechtigungen der Workstation-Benutzer
	Zentraler Zeitplan für den Start von Aufgaben auf den Workstations, die diese Einstellung von der Gruppe vererben, falls diese primär ist. Die Einstellung des Zeitplans für Gruppen ist der Einstellung des zentralen Zeitplans für Workstations ähnlich.	Aufgaben für Workstations planen
	Lizenzschlüssel für die Workstations, für die diese Gruppe primär ist.	Lizenzmanager
	Einschränkungen für die Aktualisierung der Antivirensoftware auf den Workstations, die diese Einstellung von der Gruppe vererben, falls diese primär ist.	Updates für Workstations einschränken
	Liste der Komponenten, die auf den Workstations installiert werden sollen, die diese Einstellung von der Gruppe vererben, falls diese primär ist. Die Liste der Komponenten für Gruppen wird ähnlich wie die Liste der Komponenten für Workstations bearbeitet.	Auswahl der zu installierenden Komponenten des Antivirenpakets
	Option für die automatische Aufnahme von Workstations in diese Gruppe. Diese Option ist nur für benutzerdefinierte Gruppen verfügbar.	Automatische Gruppenmitgliedschaft einstellen
	Einstellungen der Antivirenkomponenten. Die Einstellung der Komponenten eines Antivirenpakets für Gruppen ist der Einstellung der Komponenten für Workstations ähnlich.	Antivirenkomponenten konfigurieren

5.3. Workstations zu benutzerdefinierten Gruppen hinzufügen

Dr.Web Enterprise Security Suite bietet Ihnen die folgenden Möglichkeiten, Workstations zu benutzerdefinierten Gruppen hinzuzufügen:

1. Manuelles Hinzufügen.
2. Hinzufügen anhand der Regeln für automatische Gruppenmitgliedschaft.

5.3.1. Workstations zu Gruppen manuell hinzufügen

Workstations können zu benutzerdefinierten Gruppen über zwei Wege hinzugefügt werden:

1. Durch Änderung der Repository-Einstellungen.
2. Durch Ziehen der Workstation in der hierarchischen Liste (per Drag-and-drop).

So bearbeiten Sie die Liste von Gruppen, zu denen eine Workstation gehört, mithilfe ihrer Einstellungen

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste des geöffneten Fensters auf den Namen der gewünschten Workstation.
2. In die Einstellungen der Workstation gelangen Sie wie folgt:
   - Wählen Sie im Verwaltungsmenü den Punkt **Eigenschaften**.
   - Alternativ können Sie auf der Symbolleiste auf **Allgemein** → **Editieren** klicken.
3. Wechseln Sie im geöffneten Fenster **Eigenschaften der Station** zum Bereich **Gruppen**.

   In der Liste **Mitgliedschaft** werden Gruppen aufgeführt, denen die Workstation bereits angehört und in die sie aufgenommen werden kann.
4. Um die Workstation einer benutzerdefinierten Gruppe hinzuzufügen, aktivieren Sie das Kontrollkästchen neben dieser Gruppe in der Liste **Mitgliedschaft**.
5. Um eine Workstation aus der benutzerdefinierten Gruppe zu entfernen, deaktivieren Sie in der Liste **Mitgliedschaft** das Kontrollkästchen neben dieser Gruppe.

Workstations in den vordefinierten Gruppen können nicht entfernt werden.

6. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie auf **Speichern**.

Im Bereich **Eigenschaften** können Sie auch eine primäre Gruppe für die Workstation definieren (mehr dazu finden Sie unter Vererbung der Workstation-Konfiguration. Primäre Gruppen).

So bearbeiten Sie die Liste von Gruppen, zu denen eine Workstation gehört, mithilfe der hierarchischen Liste

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk** und erweitern Sie die hierarchische Liste von Gruppen und Workstations.
2. Um eine Workstation der gewünschten benutzerdefinierten Gruppe hinzuzufügen, halten Sie die STRG-TASTE gedrückt und ziehen Sie die Workstation mit Drag-and-Drop auf die gewünschte Gruppe.
3. Um die Workstation aus einer benutzerdefinierten Gruppe in eine andere zu verschieben, ziehen Sie diese mit Drag-and-Drop aus der Gruppe, aus der sie entfernt werden soll, auf die Gruppe, zu der diese Workstation hinzugefügt werden soll.

Beim Ziehen der Workstation aus einer vordefinierten Gruppe im Schritt 2 bzw. 3 wird diese Workstation der benutzerdefinierten Gruppe hinzugefügt. Dabei bleibt sie aber in der benutzerdefinierten Gruppe erhalten.

5.3.2. Automatische Gruppenmitgliedschaft einstellen

Dr.Web Enterprise Security Suite bietet die Möglichkeit, Regeln für die automatische Aufnahme der Workstations in benutzerdefinierte Gruppen zu definieren.

So geben Sie Regeln für die automatische Gruppenmitgliedschaft an

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie in der hierarchischen Liste des Antivirus-Netzwerks die benutzerdefinierte Gruppe, für die Sie Mitgliedschaftsregeln erstellen wollen.
3. Sie können auf den Bereich zum Bearbeiten der Mitgliedschaftsregeln über einen der folgenden Wege gelangen:
   - Wählen Sie im Verwaltungsmenü, im Bereich **Allgemein** den Punkt **Gruppenregeln**.
   - Alternativ können Sie in der Symbolleiste auf **Allgemein** → **Editieren** klicken. Klicken Sie dann im Bereich der Gruppeneigenschaften im rechten Fensterteil unter **Konfiguration** auf **Gruppenregeln**.
   - Wählen Sie im Verwaltungsmenü, im Bereich **Allgemein** den Punkt **Eigenschaften**. Wechsel Sie zur Registerkarte **Konfiguration** und klicken Sie dann auf **Gruppenregeln**.
4. Legen Sie im neu geöffneten Fenster die Bedingungen fest, unter denen Workstations zu dieser Gruppe hinzugefügt werden müssen:
   a) Wenn für diese Gruppe noch keine Mitgliedschaftsregeln definiert wurden, klicken Sie auf **Regel hinzufügen**.
   b) Legen Sie für jeden Regelsatz die folgenden Einstellungen fest:
      - Wählen Sie eine der Optionen aus, die bestimmen soll, wie die Regeln innerhalb dieses Satzes bei einer Kombination miteinander in Beziehung stehen werden: **Entspricht allen Bedingungen**, **Entspricht jeglicher der Bedingungen**, **Entspricht keiner der Bedingungen**.
      - Wählen Sie in den Dropdown-Listen der Bedingungen: einen von den Parametern der Workstation, der auf die Einhaltung der Bedingungen überprüft wird; ein Distributivprinzip für die Einhaltung dieser Bedingung, und geben Sie anschließend die Zeichenfolge der Bedingung an, sofern der Parameter der Workstation dies annimmt.
      - Um eine weitere Bedingung diesem Regelsatz hinzuzufügen, klicken Sie auf rechts von der Zeichenfolge der Bedingung.
   c) Um einen neuen Regelsatz hinzuzufügen, klicken Sie auf rechts vom Regelsatz. Legen Sie dabei fest, wie dieser Regelsatz mit den anderen Regelsätzen verknüpft werden:
      - **UND**. Bedingungen der beiden Sätze müssen gleichzeitig erfüllt werden.
      - **ODER**. Bedingungen mindestens eines Satzes müssen erfüllt werden.
5. Um die festgelegten Regeln zu speichern und zu übernehmen, klicken Sie eine der folgenden Schaltflächen an:
   - **Jetzt anwenden**. Diese Option gibt an, die festgelegten Regeln zu speichern und sie gleichzeitig für alle Workstations, die auf diesem **Server** registriert sind, anzuwenden. Wenn mit dem **Server** viele Workstations verbunden sind, kann die Ausführung dieser Aktion einige Zeit dauern. Die Regeln für die Umgruppierung der Workstations werden bei allen bereits registrierten Workstations angewendet, sobald die Aktion festgelegt ist. Sie werden dann für alle Workstations, darunter auch für die auf dem **Server** neu registrierten Workstations, angewendet, sobald sie mit ihm zum ersten Mal verbunden sind.
   - **Bei Verbindung von Stationen anwenden**. Diese Option gibt an, die festgelegten Regeln zu speichern und sie bei der Herstellung einer Verbindung mit dem **Server** anzuwenden. Die Regeln für die Umgruppierung der Workstations werden bei allen bereits registrierten Workstations angewendet, sobald sie mit dem **Server** wieder verbunden sind. Sie werden dann für alle Workstations, die auf dem **Server** das erste Mal registriert wurden, angewendet, sobald sie mit ihm zum ersten Mal verbunden sind.
6. Beim Festlegen von Regeln der automatischen Mitgliedschaft für eine benutzerdefinierte Gruppe wird neben dem Symbol dieser Gruppe in der hierarchischen Liste des Antivirus-Netzwerks das Symbol angezeigt (dafür muss das Kontrollkästchen **Das Symbol für Mitgliedschaftsregeln anzeigen** in der Liste **Einstellungen der Verzeichnisstruktur** auf der Symbolleiste aktiviert sein).

Wenn die Workstation in eine benutzerdefinierte Gruppe anhand der Mitgliedschaftsregeln automatisch verschoben wurde, hat das manuelle Löschen dieser Workstation keinen Sinn, da sie bei der nächsten Verbindung mit dem **Server** in diese Gruppe automatisch erneut verschoben wird.

So löschen Sie Regeln für die automatische Gruppenmitgliedschaft

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie in der hierarchischen Liste des Antivirus-Netzwerks eine benutzerdefinierte Gruppe, für die Sie Mitgliedschaftsregeln entfernen wollen.
3. Führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie in der Symbolleiste auf **Gruppenregeln löschen**.
   - Alternativ können Sie auf der Symbolleiste auf **Allgemein** → **Editieren** klicken. Klicken Sie dann im Bereich der Gruppeneigenschaften im rechten Fensterteil unter **Konfiguration** auf **Gruppenregeln löschen**.
   - Wählen Sie im Verwaltungsmenü, im Bereich **Allgemein** den Punkt **Eigenschaften**. Wechsel Sie zur Registerkarte **Konfiguration** und klicken Sie dann auf **Gruppenregeln löschen**.
4. Nachdem Mitgliedschaftsregeln der Gruppe gelöscht wurden, werden alle Workstations, die in diese Gruppe anhand der Mitgliedschaftsregeln verschoben wurden, gelöscht. Wenn diese Gruppe für eine der Workstations als primäre Gruppe definiert wurde, wird die Gruppe **Everyone** als primäre Gruppe für solche Workstations festgelegt.

5.4. Gruppenbasierte Konfiguration von Workstations

Die Einstellungen der Workstation können:

1. von der primären Gruppe geerbt werden,
2. oder individuell festgelegt werden.

Vererbung der Einstellungen

Bei der Erstellung einer neuen Gruppe werden ihre Einstellungen von der übergeordneten Gruppe bzw. von der Gruppe **Everyone** übernommen, wenn keine übergeordnete Gruppe festgelegt wurde.

Bei der Erstellung einer neuen Workstation werden ihre Einstellungen von der primären Gruppe geerbt.

Mehr dazu finden Sie unter Vererbung der Workstation-Konfiguration. Primäre Gruppen.

Bei der Anzeige bzw. beim Bearbeiten der Konfigurationselemente der Workstation, die von der primären Gruppe vererbt wurden, wird in den entsprechenden Fenstern angezeigt, dass diese Einstellungen von der primären Gruppe vererbt wurden.

Sie können verschiedene Konfigurationen für verschiedene Gruppen und Workstations festlegen, indem Sie Änderungen an den jeweiligen Einstellungen vornehmen.

Individuelle Einstellungen

Um individuelle Einstellungen der Workstation festzulegen, bearbeiten Sie die entsprechenden Einstellungen (mehr dazu finden Sie unter Eigenschaften der Workstation – Konfiguration). Im Bereich mit diesen Einstellungen wird dabei angezeigt, dass diese Einstellung individuell für diese Workstation festgelegt wurde.

Beim Festlegen von individuellen Einstellungen haben die Einstellungen der primären Gruppe sowie ihre eventuelle Änderung keinen Einfluss auf die Einstellungen der Workstation.

Sie können die Konfiguration, die von der primären Gruppe geerbt wurde, wiederherstellen. Klicken Sie dafür auf **Persönliche Einstellungen entfernen** auf der Symbolleiste des **Verwaltungscenters** im Bereich der entsprechenden Einstellungen bzw. im Bereich mit den Eigenschaften der Workstation.

5.4.1. Vererbung der Workstation-Konfiguration

Vererbung der Einstellungen

Bei der Erstellung einer neuen Workstation wird ihre Konfiguration von einer der Gruppen, zu denen sie gehört, übernommen. Solche Gruppe wird als *primäre* Gruppe bezeichnet.Wenn die Einstellungen der Primärgruppe geändert werden, werden die Änderungen auch von den zur Gruppe gehörigen Workstations geerbt. Eine Ausnahme sind die Workstations, für die individuelle Einstellungen festgelegt wurden. Bei der Erstellung einer Workstation können Sie angeben, welche der Gruppen als Primärgruppe festgelegt werden soll. Als Primärgruppe wird standardmäßig die Gruppe **Everyone** verwendet.

Wenn die primäre Gruppe nicht die Gruppe **Everyone** ist und die andere primäre Gruppe keine individuellen Einstellungen hat, werden die Einstellungen der Gruppe **Everyone** geerbt.

Die Vererbung der Konfiguration in verschachtelten Gruppen hängt von der Hierarchie der Gruppen ab. Wenn eine Workstation keine individuellen Einstellungen hat, vererbt sie die Konfiguration der primären Gruppe. Die Suche erfolgt rekursiv von unten nach oben die hierarchische Baumstruktur entlang. Als erste wird die primäre Gruppe der Workstation und als letzte die übergeordnete Gruppe geprüft. Wenn dabei keine individuellen Einstellungen gefunden wurden, wird die Konfiguration der Gruppe **Everyone** geerbt.

Beispiel:

Die Struktur einer hierarchischen Liste sieht so aus:

Die Gruppe `Group4` ist die primäre Gruppe für die Workstation `Station1`. Bei der Vererbung der Einstellungen durch die Workstation `Station1` erfolgt die Suche nach Einstellungen in dieser Reihenfolge: `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.

Standardmäßig wird die Struktur des Netzwerks so dargestellt, dass die Zugehörigkeit der Workstation zu allen Gruppen, zu denen sie gehört, angezeigt wird. Wenn Sie wollen, dass Workstations im Netzwerkverzeichnis nur in ihren primären Gruppen angezeigt werden, deaktivieren Sie auf der Symbolleiste des **Verwaltungscenters** unter **Einstellungen der Verzeichnisstruktur** das Kontrollkästchen **Mitgliedschaft in allen Gruppen**.

Auswahl einer primären Gruppe

Es gibt mehrere Möglichkeiten, für Workstation und eine Gruppe von Workstations eine neue primäre Gruppe festzulegen.

So legen Sie die primäre Gruppe für eine Workstation fest

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste des geöffneten Fensters auf den Namen der gewünschten Workstation.

2. Wählen Sie im Verwaltungsmenü den Punkt **Eigenschaften** oder klicken Sie auf der Symbolleiste auf **Allgemein** → **Editieren**. Wechseln Sie im geöffneten Fenster zur Registerkarte **Gruppen**.
3. Um eine andere primäre Gruppe für die Workstation festzulegen, klicken Sie im Bereich **Mitgliedschaft** auf das Symbol der gewünschten Gruppe. Auf dem Symbol der Gruppe wird dabei das Zeichen **1** angezeigt.
4. Klicken Sie auf **Speichern**.

So legen Sie die primäre Gruppe für mehrere Workstations fest

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste des geöffneten Fensters auf den Namen der gewünschten Workstations. Dabei können Sie auch Gruppen von Workstations auswählen. Im letzten Fall wird die Aktion für alle der Gruppe gehörenden Workstations ausgeführt. Eine Mehrfachauswahl ist möglich mit gedrückter STRG- bzw. UMSCHALTTASTE.
2. Klicken Sie auf der Symbolleiste auf **Allgemein** → **Primärgruppe für Stationen definieren**. Es öffnet sich das Fenster mit der Liste der Gruppen, die für diese Workstations als primäre Gruppen verwendet werden können.
3. Um die primäre Gruppe festzulegen, klicken Sie auf den Namen der gewünschten Gruppe.

Sie können eine Gruppe als primäre Gruppe für alle zu ihr gehörenden Workstations festlegen. Wählen Sie dafür im Verzeichnis die gewünschte Gruppe aus und klicken Sie auf der Symbolleiste des **Verwaltungscenters** auf **Allgemein** → **Diese Gruppe als primär definieren**.

5.4.2. Einstellungen in andere Gruppen oder Workstations kopieren

Die Konfigurationseinstellungen von Antivirenkomponenten, Zeitplänen, Benutzerrechten und anderen Einstellungen der Gruppe bzw. Workstation können in eine Gruppe bzw. mehrere Gruppen und Workstations kopiert (übertragen) werden.

So kopieren Sie die Einstellungen

1. Klicken Sie auf **Diese Einstellungen auf ein anderes Objekt verbreiten**:
   - Im Fenster zum Bearbeiten der Konfigurationseinstellungen der Antivirenkomponente.
   - Im Aufgabenplaner.
   - Im Fenster zur Konfiguration der Update-Restriktionen.
   - Im Fenster der zu installierenden Komponenten.
   - Im Fenster zur Konfiguration der Rechte der Workstation-Benutzer.

   Es öffnet sich das Fenster mit der Liste des Antivirus-Netzwerks.
2. Wählen Sie in dieser Liste die Gruppen und Workstations, auf die Sie die Einstellungen verteilen wollen.
3. Um die Änderungen an der Konfiguration dieser Gruppen zu übernehmen, klicken Sie auf **Speichern**.

5.5. Workstations und Gruppen vergleichen

Die Grundeinstellungen der Workstations und Gruppen können miteinander verglichen werden.

So vergleichen Sie mehrere Objekte des Antivirus-Netzwerks

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste des geöffneten Fensters die zu vergleichenden Objekte aus. Verwenden Sie dazu die STRG- oder UMSCHALTTASTE. Die folgenden Varianten sind möglich:
   - Wählen Sie mehrere Workstations aus, um sie zu vergleichen.
   - Wählen Sie mehrere Gruppen aus, um diese Gruppen und alle verschachtelten Gruppen zu vergleichen.
   - Wählen Sie mehrere Workstations und Gruppen aus, um alle Workstations zu vergleichen. Verglichen werden dabei die direkt in der hierarchischen Liste ausgewählten Workstations sowie Workstations, die zu allen ausgewählten Gruppen und ihren verschachtelten Gruppen gehören.
2. Klicken Sie im Verwaltungsmenü auf **Vergleich**.
3. Es öffnet sich eine Tabelle, in der ausgewählte Objekte verglichen werden.
   - Für Gruppen sind die folgenden Vergleichsoptionen verfügbar:
     - **Stationen**. Das ist die Gesamtzahl der Workstations, die zu dieser Gruppe gehören.
     - **Stationen im Netzwerk**. Das ist die Anzahl der momentan aktiven Workstations.
     - **Primärgruppe für**. Das ist die Anzahl der Workstations, für welche die ausgewählte Gruppe primär ist.
     - **Persönliche Einstellungen**. Hier werden Komponenten mit den individuellen Einstellungen angegeben, die von der übergeordneten Gruppe nicht geerbt wurden.
   - Für Workstations sind die folgenden Vergleichsoptionen verfügbar:
     - **Erstellungsdatum** der Workstation.
     - **Primärgruppe** der Workstation.
     - **Persönliche Einstellungen**. Hier werden Komponenten mit den individuellen Einstellungen angegeben, die von der primären Gruppe nicht geerbt wurden.
     - **Installierte Komponenten**. Hier werden die Antivirenkomponenten aufgelistet, die auf dieser Workstation installiert sind.

Kapitel 6: Workstations verwalten

Das durch **Dr.Web Enterprise Security Suite** gesteuerte Antivirus-Netzwerk dient u. a. zur zentralen Konfiguration von Antivirenpaketen, die auf Workstations installiert sind. **Dr.Web Enterprise Security Suite** ermöglicht:

- Parameter der Antivirenprogramme einzustellen.
- Aufgaben auf Workstations zu planen.
- Einzelne Aufgaben unabhängig von den festgelegten Zeitplaneinstellungen auf Workstations zu starten.
- Workstations zu aktualisieren bzw. erneut zu aktualisieren, wenn Fehler bei der letzten Aktualisierung aufgetreten sind (eventueller Fehlerzustand wird dabei zurückgesetzt).

Der Administrator des Antivirus-Netzwerks kann dem Benutzer der Workstation die für das Planen und Starten von Aufgaben erforderlichen Berechtigungen gewähren, sie verweigern oder wesentlich einschränken.

Die Konfiguration einer Workstation kann auch dann geändert werden, wenn keine Kommunikation zwischen ihr und dem **Server** zwischenzeitlich stattfinden kann. Die an der Workstation vorgenommenen Änderungen werden übernommen, sobald eine Verbindung mit dem **Server** hergestellt ist.

6.1. Workstation-Konten verwalten

6.1.1. Verbindungsrichtlinie für Workstations

Die Erstellung von Workstations über das **Verwaltungscenter** wird in der **Installationsanleitung** unter Neues Konto erstellen detailliert beschrieben.

Die Autorisierungsverwaltung auf dem **Dr.Web Server** hängt jeweils vom Folgenden ab:

1. Wenn das Kontrollkästchen **Manuelle Autorisierung auf dem Server** bei der Installation des **Agents** auf der Workstation deaktiviert wurde, sind für den Zugriff der Workstation auf den **Server** die Einstellungen entscheidend, die auf dem **Server** (standardmäßig verwendet) festgelegt wurden. Mehr dazu finden Sie unten.
2. Wenn das Kontrollkästchen **Manuelle Autorisierung auf dem Server** bei der Installation des **Agents** auf der Workstation aktiviert wurde, und die Einstellungen **Identifikator** und **Passwort** festgelegt wurden, wird die Workstation bei der Verbindung mit dem **Server** unabhängig von den Einstellungen des **Servers** automatisch autorisiert (diese Methode wird standardmäßig verwendet, wenn der **Agent** mithilfe des Installationspakets *drweb-esuite-install* installiert wurde. S. dazu auch die **Installationsanleitung**, den Punkt Installationsdateien).

Das Festlegen des Autorisierungstyps bei der Installation des **Agents** wird im **Benutzerhandbuch** detailliert beschrieben.

So ändern Sie den Modus für den Zugriff auf den Dr.Web Server

1. Wechseln Sie zu den Einstellungen des **Servers**. Wählen Sie dafür im Hauptmenü den Punkt **Administrierung**. Wählen Sie dann im Verwaltungsmenü den Punkt **Dr.Web Server-Konfiguration**.

2. Wählen Sie auf der Registerkarte **Allgemein** in der Dropdown-Liste **Registrierung der Anfänger** eine der folgenden Optionen aus:
   - **Manuelle Zugriffsbestätigung** (dieser Modus wird standardmäßig verwendet, wenn bei der Installation des **Servers** kein anderer Modus ausgewählt wurde).
   - **Zugriff immer verweigern**.
   - **Zugriff automatisch erlauben**.

Manuelle Zugriffsbestätigung

Im Modus **Manuelle Zugriffsbestätigung** werden neue Workstations in die Untergruppe **Newbies** der Gruppe **Status** verschoben, bis der Administrator sie genehmigt.

So steuern Sie den Zugriff für nicht bestätigte Workstations

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste Workstations in der Untergruppe **Newbies** der Gruppe **Status** aus.
2. Um einen Modus für den Zugriff auf den **Server** anzugeben, legen Sie in Bereich **Nicht bestätigte Stationen** eine Aktion fest, die für die ausgewählten Workstations angewendet wird:

   Zugriff für die ausgewählten Stationen erlauben und Gruppe als primär definieren. Erzwingt die Bestätigung des Zugriffs der Workstation auf den **Server** und Festlegung einer Primärgruppe aus der vorhandenen Liste.

   Die zur Ausführung definierte Aktion beim Verbindungsaufbau zurücksetzen. Erzwingt den Abbruch der Aktion für eine nicht bestätigte Workstation, die bei der Verbindung der Workstation mit dem **Server** ausgeführt werden sollte.

   Ausgewählten Stationen Zugriff verbieten. Verweigert der Workstation den Zugriff auf den **Server**.

Zugriffsverweigerung

Im Modus **Zugriff immer verweigern** verweigert der **Server** allen neuen Workstations den Zugriff. Der Administrator muss dann für diese Workstations neue Einträge manuell erstellen und ihnen Passwörter vergeben.

Automatischer Zugriff

Im Modus **Zugriff automatisch erlauben** stellen alle Workstations, die Zugriff auf den **Server** anfordern, eine Verbindung automatisch her, ohne weitere Anforderungen an den Administrator zu versenden. Als primäre Gruppe wird dabei die Gruppe verwendet, die in der Dropdown-Liste **Primärgruppe** unter **Dr.Web Server-Konfiguration** auf der Registerkarte **Allgemein** festgelegt wurde.

6.1.2. Workstation löschen und wiederherstellen

Workstations löschen

So löschen Sie einen Workstation-Eintrag

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Klicken Sie dann auf der Symbolleiste auf **Allgemein** → **Ausgewählte Objekte entfernen**.
2. Klicken Sie zur Bestätigung auf **OK**.

Die aus der hierarchischen Liste entfernten Workstations werden in die Tabelle der gelöschten Workstations verschoben. Bei Bedarf können Sie die hier aufgelisteten Objekte über das **Verwaltungscenter** jederzeit wiederherstellen.

Workstation wiederherstellen

So stellen Sie einen Workstation-Eintrag wieder her

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Wählen Sie dann in der hierarchischen Liste eine bzw. mehrere gelöschte Workstations, die Sie wiederherstellen wollen.

   Alle gelöschten Workstations befinden sich in der Untergruppe **Deleted** der Gruppe **Status**.

2. Wählen Sie auf der Symbolleiste den Punkt **Allgemein** → **Gelöschte Workstations wiederherstellen**.
3. Es öffnet sich der Bereich, in dem Sie die gewünschten Workstations wiederherstellen können. Sie können dabei die folgenden Einstellungen festlegen:
   - **Primärgruppe**. Wählen Sie eine primäre Gruppe, zu der die wiederherzustellende Workstation hinzugefügt werden soll. Standardmäßig wird die primäre Gruppe ausgewählt, die der Workstation beim Löschen zugewiesen wurde.

     Wenn mehrere Workstations gleichzeitig wiederhergestellt werden sollen, wird standardmäßig die Option **Ehemalige Primärgruppe**, gewählt. Das bedeutet, dass jede der ausgewählten Workstations derjenigen primären Gruppe zugewiesen wird, der sie vor dem Löschen angehörte. Wenn eine bestimmte Gruppe ausgewählt wird, werden alle wiederherzustellenden Workstations der gleichen Gruppe zugewiesen.

   - Im Bereich **Mitgliedschaft** können Sie die Liste von Gruppen ändern, in welche die Workstation aufgenommenen werden soll. Standardmäßig sind alle Gruppen aufgelistet, denen die jeweilige Workstation vor dem Löschen gehörte. In der Liste **Mitgliedschaft** sind alle Gruppen aufgeführt, denen die Workstation zugewiesen werden kann. Aktivieren Sie die Kontrollkästchen neben den Gruppen, in welche die Workstation aufgenommen werden soll.
4. Um eine Workstation mit bereits festgelegten Parametern wiederherzustellen, klicken Sie auf **Wiederherstellen**.

6.1.3. Workstations zusammenfassen

Aufgrund von eventuellen Änderungen in der Datenbank bzw. bei der erneuten Installation der Software von Workstations werden in der hierarchischen Liste des Antivirus-Netzwerks möglicherweise mehrere Workstations mit dem gleichen Namen erstellt, obwohl nur eine von denen der jeweiligen Workstation entspricht.

So entfernen Sie Workstations mit dem gleichen Namen

1. Wählen Sie alle wiederholten Namen der Workstation aus. Verwenden Sie dafür die STRG-TASTE.
2. Wählen Sie auf der Symbolleiste **Allgemein** → **Stationen vereinigen**.
3. Wählen Sie in der Spalte die Workstation aus, die als Hauptworkstation auftreten wird. Die restlichen Workstations werden gelöscht, und deren Daten werden von der ausgewählten Workstation übernommen.
4. Wählen Sie in der Spalte eine Workstation aus, deren Einstellungen von der gewählten Hauptworkstation übernommen werden sollen.
5. Klicken Sie auf **Speichern**.

6.2. Allgemeine Einstellungen der Workstation

6.2.1. Eigenschaften der Workstation

Eigenschaften der Workstation

So bearbeiten Sie die Eigenschaften einer Workstation

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Bereich **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste des geöffneten Fensters eine Workstation aus.
2. In die Eigenschaften der Workstation gelangen Sie wie folgt:
   a) Klicken Sie auf **Allgemein** → **Editieren** auf der Symbolleiste. Die Eigenschaften der Workstation werden im rechten Bereich des **Verwaltungscenters** angezeigt.
   b) Wählen Sie im Verwaltungsmenü den Punkt **Eigenschaften**. Es öffnet sich ein Fenster mit den Eigenschaften der Workstation.
3. Dieses Fenster enthält die folgenden Gruppen der Einstellungen: **Allgemein**, **Konfiguration**, **Gruppen**, **Sicherheit**, **Standort**. Diese Einstellungen werden im Nachfolgenden beschrieben.
4. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie auf **Speichern**.

Individuelle Einstellungen der Workstation löschen

So löschen Sie die individuellen Einstellungen einer Workstation

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Bereich **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste des geöffneten Fensters eine Workstation aus und klicken Sie in der Symbolleiste auf **Allgemein** → **Persönliche Einstellungen entfernen**. Alle Einstellungen der Workstation werden angezeigt. Individuelle Einstellungen werden dabei durch aktivierte Kontrollkästchen gekennzeichnet.
2. Deaktivieren Sie die Kontrollkästchen bei den Einstellungen, die entfernt werden sollen. Klicken Sie dann auf **Löschen**. Die Einstellungen der Workstation, die von der primären Gruppe geerbt wurden, werden wiederhergestellt.

Bevor Sie mit der Konfiguration einer Workstation für Komponenten **SpIDer Guard für Windows** sowie **Dr.Web Scanner für Windows** beginnen, machen Sie sich mit den Empfehlungen zum Verwenden der Antivirenprogramme auf den Rechnern unter Windows Server 2003 und Windows XP vertraut. Der entsprechende Artikel kann unter http://support.microsoft.com/kb/822158/de abgerufen werden. Dieser Artikel enthält Informationen dazu, wie Sie die Systemleistung optimieren können.

Falls Ihr Schlüssel für den **Agent** (`agent.key`) die Verwendung des Spamfilters für Komponente **SpIDer Mail** zulässt, können Sie auf der Registerkarte **Antispam** den Filter einstellen. Wählen Sie dafür im Kontextmenü einer beliebigen Gruppe bzw. Workstation den Punkt **SpIDer Mail für Workstations**.

Ab Version **5.0** gehören zum Leistungsumfang von **Dr.Web Enterprise Security Suite** die Komponenten **SpIDer Gate** und **Office Control** . Diese Komponenten können aber nur dann verwendet werden, wenn sie in Ihrer Lizenz (**Antivirus + Antispam**) angegeben sind. Die Lizenz kann im Schlüssel des **Agents** eingesehen werden.

Einstellungen des Spamfilters sowie der Komponenten **SpIDer Gate** und **Office Control** werden im Handbuch **Dr.Web Agent® für Windows. Benutzerhandbuch** detailliert beschrieben.

6.2.1.1. Allgemein

Der Bereich **Allgemein** enthält die folgenden schreibgeschützten Felder:

- **Identifikator der Workstation**. Die eindeutige ID der Workstation.
- **Name**. Der Name der Workstation.
- **Erstellungsdatum**. Das Datum der Erstellung der Workstation auf dem **Server**.
- **Ende des Kostenlosen Nutzungszeitraums**. Das Datum, bis zu dem der **Antivirus** auf der Workstation kostenlos genutzt werden darf.

Sie können Werte in den folgenden Feldern festlegen bzw. ändern:

- Legen Sie im Feld **Passwort** das Passwort für die Autorisierung der Workstation auf dem **Server** fest (wiederholen Sie das Passwort im Feld **Passwort bestätigen**). Beim Passwortwechsel wiederholen Sie auf der Workstation dieses Verfahren in den Verbindungseinstellungen des **Agents**, um die Verbindung mit dem **Agent** zu ermöglichen.
- Geben Sie im Feld **Beschreibung** zusätzliche Informationen zur Workstation an.

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

Dieser Abschnitt beinhaltet auch die folgenden Links:

- Unter dem Punkt **Installationsdatei** finden Sie den Link zum Herunterladen vom Installationsprogramm des **Agents** für die Workstation.

  Sobald die Workstation erstellt ist, aber bevor Sie das jeweilige Betriebssystem der Workstation angeben müssen, werden Ihnen im Bereich zum Herunterladen der Distribution Links für jedes der von **Dr.Web Enterprise Security Suite** unterstützten Betriebssysteme zur Verfügung gestellt.

- Unter dem Punkt **Konfigurationsdatei** finden Sie einen Link zum Herunterladen der Datei mit den Einstellungen für die Verbindung von Workstations unter Android, MAC OS X und Linux mit dem **Dr.Web Server**.

6.2.1.2. Konfiguration

Im Bereich **Konfiguration** können Sie die Konfiguration von Workstations ändern. Die Konfiguration besteht aus den folgenden Parametern:

Symbol	Einstellungen	Abschnitt mit der Beschreibung
	Rechte des Workstation-Benutzers	Berechtigungen der Workstation-Benutzer
	Zeitgesteuerter Start von Aufgaben auf der Workstation	Aufgaben für Workstations planen
	Lizenzschlüssel für die Workstation	Lizenzmanager
	Einschränkungen für die Aktualisierung der Antivirensoftware	Updates für Workstations einschränken
	Liste der zu installierenden Komponenten	Auswahl der zu installierenden Komponenten des Antivirenpakets
	Einstellungen der Komponenten des Antivirenpakets der Workstation	Antivirenkomponenten konfigurieren

Über das **Verwaltungscenter** können Sie auch die individuellen Einstellungen der Workstation löschen. Die entsprechenden Schaltflächen befinden sich rechts von den Konfigurationsschaltflächen. Nach dem Löschen der individuellen Einstellungen der Workstation wird die von der primären Gruppe geerbte Konfiguration verwendet.

Bei der Änderung der Einstellungen von **SpIDer Gate** und/oder **Office Control Control** müssen Sie beachten, dass die Einstellungen beider Komponenten untereinander verknüpft sind: Wenn die Einstellungen einer Komponente über die Schaltfläche **Persönliche Einstellungen entfernen** gelöscht werden, werden ebenfalls die Einstellungen der anderen Komponente gelöscht. In diesem Fall werden die von der übergeordneten Gruppe geerbten Einstellungen verwendet.

6.2.1.3. Gruppen

Im Bereich **Gruppen** wird die Liste der Gruppen festgelegt, zu denen die Workstation gehört. In der Liste **Mitgliedschaft** werden Gruppen aufgeführt, denen die Workstation bereits angehört und in die sie aufgenommen werden kann.

So ändern Sie die Mitgliedschaft einer Workstation

1. Um eine Workstation zur benutzerdefinierten Gruppe hinzuzufügen, aktivieren Sie in der Liste **Mitgliedschaft** das Kontrollkästchen neben dieser Gruppe.
2. Um eine Workstation aus der benutzerdefinierten Gruppe zu entfernen, deaktivieren Sie in der Liste **Mitgliedschaft** das Kontrollkästchen neben dieser Gruppe.

Workstations in den vordefinierten Gruppen können nicht entfernt werden.

3. Um eine andere primäre Gruppe für die Workstation festzulegen, klicken Sie in der Liste **Mitgliedschaft** auf das Symbol der gewünschten Gruppe. Auf dem Symbol der Gruppe wird dabei das Zeichen **1** angezeigt.

6.2.1.4. Sicherheit

Im Bereich **Sicherheit** werden Einschränkungen für Netzwerkadressen festgelegt, die der auf der Workstation installierte **Agent** zur Verbindung mit dem **Server** verwenden kann.

Um alle Verbindungen zu erlauben, deaktivieren Sie das Kontrollkästchen **Diese Zugriffssteuerungsliste verwenden**. Um eine Liste der zugelassenen bzw. verbotenen Adressen zusammenzustellen, aktivieren Sie dieses Kontrollkästchen.

Um eine TCP-Adresse zuzulassen, fügen Sie diese der Liste **TCP: Erlaubt** oder **TCPv6: Erlaubt** hinzu.

Um eine TCP-Adresse zu verbieten, fügen Sie diese der Liste **TCP: Verboten** oder **TCPv6: Verboten** hinzu.

So bearbeiten Adressen in der Liste

1. Geben Sie ins entsprechende Feld die Netzwerkadresse im folgenden Format ein: *<IP-Adresse>*/[*<Netzwerkpräfix>*].
2. Um ein neues Feld hinzuzufügen, klicken Sie im entsprechenden Bereich auf die Schaltfläche .
3. Um ein Feld zu löschen, klicken Sie auf neben der zu löschenden Adresse.
4. Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**.

Beispiel für einen Präfix:

1. Das Präfix 24 steht für Netzwerke mit einer Subnetzmaske: `255.255.255.0`

   Beinhaltet 254 Adressen

   Hostadressen in diesen Netzwerken sehen so aus: `195.136.12.*`

2. Das Präfix 8 steht für Netzwerke mit einer Subnetzmaske: `255.0.0.0`

   Beinhaltet bis zu 16387064 Adressen (256*256*256)

   Hostadressen in diesen Netzwerken sehen so aus: `125.*.*.*`

Außerdem können Sie Adressen aus der Liste löschen und hinzugefügte Adressen bearbeiten.

Adressen, die keiner der Listen hinzugefügt wurden, werden je nach dem, ob das Kontrollkästchen **Priorität des Verbots** aktiviert ist, zugelassen oder verboten. Wenn das Kontrollkästchen aktiviert ist, hat die Liste **Verboten** Vorrang gegenüber der Liste **Erlaubt**. Adressen, die keiner Liste bzw. beiden Listen hinzugefügt sind, werden nicht zugelassen. Erlaubt sind nur Adressen, die der Liste **Erlaubt** hinzugefügt sind und nicht in der Liste **Verboten** vorhanden sind.

6.2.1.5. Stelle

Im Bereich **Stelle** können Sie zusätzliche Informationen über den physischen Standort der Workstation angegeben.

Darüber hinaus wird hier die Lage der Workstation auf der geographischen Karte angezeigt.

So lassen Sie die Lage einer Workstation auf der Karte anzeigen

1. Geben Sie in den Feldern **Breite** und **Länge** die geographischen Koordinaten der Workstation in Dezimalgrad (Decimal Degrees) an.
2. Um die eingegebenen Daten zu speichern, klicken Sie auf **Speichern**.
3. Auf der Registerkarte **Stelle** wird die Vorschau von OpenStreetMaps mit der Markierung des festgelegten Standorts angezeigt.

   Wenn die Vorschau nicht geladen werden kann, erscheint der Text **Auf der Karte anzeigen**.

4. Um die Karte in voller Größe anzeigen zu lassen, klicken Sie auf die Vorschau oder den Text **Auf der Karte anzeigen**.

6.2.2. Installierte Komponenten des Antivirenpakets

Komponenten

So lassen Sie die auf einer Workstation installierten Komponenten anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
2. Wählen Sie im geöffneten Verwaltungsmenü unter dem Unterbereich **Allgemein** den Punkt **Installierte Komponenten**.
3. Im geöffneten Fenster werden Informationen über die installierten Komponenten angezeigt. Darunter fallen der Name der Komponente; Datum und Uhrzeit der Installation; Adresse des **Servers**, von dem her diese Komponente installierte wurde; Installationsverzeichnis der Komponente auf der Workstation.

Der Umfang der installierten Komponenten hängt jeweils vom Folgenden ab:

- Von den gemäß dem Lizenzschlüssel erlaubten Komponenten.
- Vom jeweiligen Betriebssystem der Workstation.
- Von den Einstellungen, die durch den Administrator auf dem **Server** des Antivirus-Netzwerks festgelegt wurden. Der Administrator kann den Umfang von Komponenten des Antivirenpakets der Workstation sowohl vor der Installation des **Agents** als auch jederzeit nach der Installation ändern (s. dazu Auswahl der zu installierenden Komponenten des Antivirenpakets).

Falls möglich, vermeiden Sie es, die Komponenten **SpIDer Gate**, **SpIDer Mail** und **Dr.Web Firewall** auf den Servern zu installieren, die wichtige Netzwerkfunktionen (z.B. Funktion eines Domänencontrollers oder Lizenz-Verteilungsservers usw.) übernehmen. Dadurch können Sie eventuelle Konflikte zwischen Netzwerkdiensten und internen Komponenten vom **Dr.Web** Antivirenprogramm verhindern.

Virendatenbanken

So lassen Sie die auf einer Workstation installierten Virendatenbanken anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation.
2. Wählen Sie im geöffneten Verwaltungsmenü unter dem Unterbereich **Statistik** den Punkt **Virendatenbanken**.
3. Es öffnet sich das Fenster, in dem Informationen über die installierten Virendatenbanken angezeigt werden. Darunter fallen der Name der Virendatenbankdatei, Version der Virendatenbank, Datum der Erstellung der Virendatenbank, Anzahl der Signaturen.

Wenn die Anzeige des Punkts **Virendatenbanken** deaktiviert ist, können Sie diese erneut aktivieren. Wählen Sie dafür im Hauptmenü den Punkt **Administrierung**. Wählen Sie dann im Verwaltungsmenü den Punkt **Dr.Web Server-Konfiguration**. Aktivieren Sie auf der Registerkarte **Statistik** die Kontrollkästchen **Status der Virendatenbanken** und **Status der Workstations**. Starten Sie abschließend den **Server** neu.

6.2.3. Hardware und Software auf Workstations unter Windows®

Dr.Web Enterprise Security Suite erlaubt es Ihnen, Informationen zur Hardware und Software von Workstations unter Windows zusammenzufassen und einzusehen.

So sammeln Sie Informationen zur Hardware und Software von Workstations

1. Aktivieren Sie auf dem **Server** das Zusammenstellen von Statistikinformationen:
   a) Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
   b) Wählen im Verwaltungsmenü den Punkt **Dr.Web Server-Konfiguration**.
   c) Öffnen Sie in den Einstellungen des **Servers** die Registerkarte **Statistik** und aktivieren Sie das Kontrollkästchen **Hardware und Software**, falls es deaktiviert ist.
   d) Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern** und starten Sie den **Server** neu.
2. Lassen Sie auf Workstations das Zusammenstellen von Statistikinformationen zu:
   a) Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
   b) Wählen Sie in der hierarchischen Liste eine Workstation oder Gruppe von Workstation, für die Sie das Zusammenstellen von Statistikinformationen erlauben wollen. Achten Sie bei der Auswahl einer Workstation auf die Vererbung der Einstellungen: Wenn Workstations der ausgewählten Gruppe individuelle Einstellungen haben, bleiben diese Einstellungen bei der Änderung der Gruppeneinstellungen erhalten.
   c) Wählen Sie im Verwaltungsmenü, im Bereich **Konfiguration** → **Windows** den Punkt **Dr.Web Agent**.
   d) Aktivieren Sie in den Einstellungen des **Agents** auf der Registerkarte **Allgemein** das Kontrollkästchen **Informationen zu Stationen sammeln**, falls es deaktiviert ist. Passen Sie bei Bedarf den Wert der Option **Zeitabstand für das Sammeln von Informationen über Stationen (Min.)** an.
   e) Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**. Die Einstellungen werden an Workstations übertragen.

So lassen Sie Informationen zur Hardware und Software einer Workstations anzeigen

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie in der hierarchischen Liste des Antivirus-Netzwerks die gewünschte Workstation.
3. Wählen Sie im Verwaltungsmenü, im Bereich **Allgemein** den Punkt **Hardware und Software**.
4. Im geöffneten Fenster wird eine Baumstruktur mir der Liste der auf der Workstation installierten Hardware und Software angezeigt. Ihnen stehen die folgenden Informationen zur Verfügung:
   - **Application**. Hier werden alle auf der Workstation installierten Programme aufgelistet.
   - **Hardware**. Hier wird die Liste der auf der Workstation installierten Hardware angezeigt.
   - **Operating System**. Hier finden Sie Informationen zum Betriebssystem der Workstation.
   - **Windows Management Instrumentation**. Hier werden Informationen zu Windows-Verwaltungsinstrumentation angezeigt.
5. Um die Details des gewünschten Objekts anzuzeigen, wählen Sie dieses in der Baumstruktur aus.

So lassen Sie Hardware und Software mehrerer Workstations vergleichen

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie in der hierarchischen Liste mehrere Workstations oder Gruppen von Workstations aus. Damit die Vergleichsseite angezeigt werden kann, müssen Sie mindestens zwei Workstations unter Windows auswählen.
3. Wählen Sie im Verwaltungsmenü, im Bereich **Allgemein** den Punkt **Vergleich der Hardware und Software**.
4. Im geöffneten Fenster finden Sie die folgenden Informationen:

- Liste der auf der Workstation installierten Hardware und Software.
- Tabelle, in der die von Ihnen ausgewählten Workstations miteinander verglichen werden.

5. Um die zu vergleichenden Daten anzuzeigen, wählen Sie den gewünschten Punkt in der Baumstruktur der Hardware und Software. Alle verfügbaren Werte des gewählten Punkts werden in der Vergleichsbaumstruktur dargestellt.

6.3. Workstation konfigurieren

6.3.1. Berechtigungen der Workstation-Benutzer

So bearbeiten Sie die Berechtigungen von Workstation-Benutzern über das Dr.Web Sicherheitscenter

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste des geöffneten Fensters auf den Namen der gewünschten Workstation. Wählen Sie im geöffneten Verwaltungsmenü den Punkt **Rechte**. Es öffnet sich das Fenster zum Bearbeiten der Berechtigungen.
2. Die Berechtigungen werden auf der Registerkarte, die dem jeweiligen Betriebssystem der Workstation entspricht, bearbeitet. Um eine Berechtigung zu gewähren oder zu verweigern, aktivieren bzw. deaktivieren Sie das Kontrollkästchen neben dieser Berechtigung.
3. Die Bearbeitung der Berechtigungen für Workstations unter Windows, MAC OS X, Linux und Android erfolgt auf den folgenden Registerkarten:
   - **Komponenten**. Hier werden Berechtigungen zur Verwaltung von Antivirenkomponenten bearbeitet. Standardmäßig kann der Benutzer jede der Komponenten starten. Ihm ist aber verboten, die Konfiguration der Komponenten zu ändern und die Komponenten zu deaktivieren.
   - **Allgemein**. Hier werden Berechtigungen zur Verwaltung des **Dr.Web Agents** und seiner Funktionen bearbeitet:

Tabelle 6-1: Festlegen der Berechtigungen auf der Registerkarte Allgemein

Kontrollkästchen im Bereich	Aktion des Kontrollkästchens	Ergebnis auf der Workstation bei Deaktivierung des Kontrollkästchens
Workstations unter Windows		
Im Mobilmodus starten	Aktivieren Sie das Kontrollkästchen, um Benutzern der Workstation zu erlauben, in den mobilen Modus zu wechseln und Updates direkt über das **Dr.Web Globale Update-System** zu erhalten, wenn keine Verbindung mit dem **Dr.Web Server** besteht.	In den Einstellungen des **Agents** unter **Allgemein** > **Modus** ist die Option **Mobilmodus nutzen, wenn keine Verbindung zum Server besteht** nicht mehr verfügbar.
Funktionsmodus bearbeiten	Aktivieren Sie das Kontrollkästchen, damit Benutzer der Workstation zwischen den Betriebsmodi des **Dr.Web Agents** wechseln können.	In den Einstellungen des **Agents** unter **Allgemein** > **Modus** sind folgende Einstellungen nicht mehr verfügbar: • **Updates vom Server erhalten**. • **Aufgaben vom Server erhalten**. • **Ereignisse speichern**.
Konfiguration des Dr.Web Agenten ändern	Aktivieren Sie das Kontrollkästchen, damit Benutzer der Workstation die Einstellungen des **Dr.Web Agents** ändern können.	In den Einstellungen des **Agents** unter **Allgemein** > Modus sind die Einstellungen folgender Unterbereiche nicht mehr verfügbar: • **Benachrichtigungen**: Keine Einstellungen verfügbar.

Kontrollkästchen im Bereich	Aktion des Kontrollkästchens	Ergebnis auf der Workstation bei Deaktivierung des Kontrollkästchens
		• **Modus**: Einstellungen für die Verbindung mit dem **Server** und das Kontrollkästchen **Systemzeit mit Serverzeit synchronisieren** nicht mehr verfügbar. • **Selbstschutz**: Die Optionen **Ändern des Systemdatums bzw. der Systemzeit verbieten**, **Emulation von Benutzer-Aktionen sperren** sind nicht mehr verfügbar. • **Erweitert**: In den Einstellungen des **Protokolls** sind die Optionen **Dr.Web Update**, **Dr.Web Services**, **Speicherauszüge bei Scan-Fehlern erstellen** nicht mehr verfügbar.
Konfiguration des Präventivschutzes ändern	Aktivieren Sie das Kontrollkästchen, damit Benutzer der Workstation Einstellungen des Präventivschutzes bearbeiten können.	In den Einstellungen des **Agents** unter **Schutzmodule** > **Präventivschutz** sind keine Einstellungen verfügbar.
Selbstschutz deaktivieren	Aktivieren Sie das Kontrollkästchen, damit Benutzer der Workstation den Selbstschutz deaktivieren können.	In den Einstellungen des **Agents** unter **Allgemein** > **Selbstschutz** ist die Option **Selbstschutz aktivieren** nicht mehr verfügbar.
Dr.Web Agenten deinstallieren	Aktivieren Sie das Kontrollkästchen, damit Benutzer der Workstation den **Dr.Web Agent** deinstallieren können.	Die Option verbietet, den **Agent** auf der Workstation mithilfe des Installationsprogramms oder mit Windows-Bordmitteln zu deinstallieren. In diesem Fall lässt sich der **Agent** nur über den Punkt **Allgemein** → **Dr.Web Agent deinstallieren** in der Symbolleiste des **Verwaltungscenters** deinstallieren.
Workstations unter Mac OS X		
Im Mobilmodus starten	Aktivieren Sie das Kontrollkästchen, um Benutzern der Workstation zu erlauben, in den mobilen Modus zu wechseln und Updates direkt über das **Dr.Web Globale Update-System** zu erhalten, wenn keine Verbindung mit dem **Dr.Web Server** besteht.	Der Bereich **Update** im Hauptfenster des Programms ist gesperrt.
Workstations unter Linux-artigen Betriebssystemen		
Im Mobilmodus starten	Aktivieren Sie das Kontrollkästchen, um Benutzern der Workstation zu erlauben, in den mobilen Modus zu wechseln und Updates direkt über das **Dr.Web Globale Update-System** zu erhalten, wenn keine Verbindung mit dem **Dr.Web Server** besteht.	Für Konsolen-Version: Der Befehl `drweb-ctl update` zum Update von Virendatenbanken über das **GUS** ist nicht mehr verfügbar.
Workstations unter Android		
Im Mobilmodus starten	Aktivieren Sie das Kontrollkästchen, um Benutzern von mobilen Geräten zu erlauben, in den mobilen Modus zu wechseln und Updates direkt über das **Dr.Web Globale Update-System** zu erhalten, wenn keine Verbindung mit dem **Dr.Web Server** besteht.	Der Bereich **Update** auf dem Hauptbildschirm der App ist gesperrt.

Wenn einer der Punkte, die für die Änderung der Einstellungen des **Agents** relevant sind, deaktiviert wird, wird jeweils der zuletzt festgelegte Wert verwendet.

Die Aktionen der entsprechenden Menüpunkte werden im Handbuch **Dr.Web für Windows. Benutzerhandbuch** detailliert beschrieben.

4. Sie können diese Einstellungen an ein anderes Objekt verteilen, indem Sie auf **Diese Einstellungen auf ein anderes Objekt verbreiten** klicken.
5. Um diese Einstellungen in eine Datei zu exportieren, klicken Sie auf **Einstellungen aus diesem Bereich in die Datei exportieren**.
6. Um diese Einstellungen aus einer Datei zu importieren, klicken Sie auf **Einstellungen aus der Datei in diesen Bereich importieren**.
7. Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**.

Wenn keine Verbindung mit dem **Server** bei der Bearbeitung der Einstellungen der Workstation besteht, werden die Einstellungen erst dann übernommen, sobald die Kommunikation zwischen dem **Agent** und **Server** wiederhergestellt ist.

6.3.2. Aufgaben für Workstations planen

Dr.Web Enterprise Security Suite bietet die Möglichkeit, *zentralen Aufgabenzeitplan* zu verwenden. Der Zeitplan wird vom Administrator des Antivirus-Netzwerks eingerichtet und entspricht allen Regeln für die Konfigurationsvererbung.

Der *Aufgabenzeitplan* ist eine Liste der Aktionen, die auf Workstations zu bestimmten Zeitpunkten automatisch ausgeführt werden. Zeitpläne dienen grundsätzlich dazu, Workstations auf Viren zum gewünschten Zeitpunkt zu scannen, ohne dass der **Scanner** manuell gestartet werden muss. Außerdem ermöglicht der **Dr.Web Agent** die Ausführung der Aktionen, die im Nachfolgenden beschrieben werden.

Die Bearbeitung des zentralen Aufgabenzeitplans erfolgt über das **Verwaltungscenter**.

So bearbeiten Sie den zentralen Aufgabenzeitplan

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe. Wählen Sie im geöffneten Verwaltungsmenü den Punkt **Aufgabenplaner**. Die Liste mit geplanten Aufgaben wird angezeigt.

Der Zeitplan für Workstations unter Windows enthält standardmäßig die Aufgabe **Daily scan** – Workstation täglich scannen (verboten).

2. Zur Verwaltung des Zeitplans werden die folgenden Elemente in der Symbolleiste verwendet:

a) Allgemeine Elemente der Symbolleiste dienen zur Erstellung neuer Aufgaben und zur allgemeinen Verwaltung des Zeitplans. Diese Tools sind jederzeit auf der Symbolleiste verfügbar.

Aufgabe erstellen – fügt eine neue Aufgabe hinzu. Mehr Information zu dieser Aktion finden Sie unten, im Unterabschnitt Aufgaben-Editor.

Diese Einstellungen auf ein anderes Objekt verbreiten – kopiert Aufgaben im Zeitplan in andere Objekte, beispielsweise in Workstations und Gruppen. Mehr Information zu dieser Aktion finden Sie im Abschnitt Einstellungen in andere Gruppen oder Workstations kopieren.

Einstellungen aus diesem Bereich in die Datei exportieren – exportiert den Zeitplan in eine Datei im speziellen Format.

Einstellungen aus der Datei in diesen Bereich importieren – importiert den Zeitplan aus einer Datei im speziellen Format.

b) Um bereits bestehende Aufgaben zu verwalten, aktivieren Sie die Kontrollkästchen neben den gewünschten Aufgaben oder in der Überschrift der Tabelle, falls alle Aufgaben in der Liste ausgewählt werden müssen. Die Elemente zur Verwaltung von ausgewählten Aufgaben werden dabei auf der Symbolleiste verfügbar.

Tabelle 6-2: Symbolleistenelemente zur Verwaltung von ausgewählten Aufgaben

Einstellung		Aktion
Status	**Ausführung erlauben**	Ausführung von ausgewählten Aufgaben nach dem festgelegten Zeitplan aktivieren, falls sie verboten wurden.
	Ausführung verbieten	Ausführung von ausgewählten Aufgaben verbieten. Aufgaben bleiben dabei in der Liste erhalten, werden aber nicht ausgeführt.
Die gleiche Aktion kann alternativ im Aufgabeneditor auf der Registerkarte **Allgemein** durch Aktivieren des Kontrollkästchens **Ausführung erlauben** durchgeführt werden.		
Schweregrad	**Kritisch machen**	Die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Agents** erzwingen, falls die geplante Ausführung versäumt wurde.
	Nicht kritisch machen	Die Aufgabe nur zum festgelegten Zeitpunkt ausführen, also unabhängig davon, ob die Ausführung der Aufgabe versäumt wurde.
Die gleiche Aktion kann alternativ im Aufgabeneditor auf der Registerkarte **Allgemein** durch Aktivieren des Kontrollkästchens **Kritische Aufgabe** durchgeführt werden.		
Einstellungen duplizieren		Die in der Liste des aktuellen Zeitplans gewählten Aufgaben duplizieren. Beim Aktivieren der Option **Einstellungen duplizieren** werden neue Aufgaben mit den Einstellungen erstellt, die den gewählten Aufgaben entsprechen.
Wiederholt planen		Diese Option gilt nur für einmalige Aufgaben: die Aufgabe noch einmal entsprechend den festgelegten Zeiteinstellungen ausführen lassen. Informationen zur Anzahl der Aufgabenausführung finden Sie im Unterabschnitt Aufgabeneditor.
Ausgewählte Aufgaben löschen		Ausgewählte Aufgabe aus dem Zeitplan entfernen.

3. Um die Parameter einer Aufgabe zu bearbeiten, wählen Sie diese in der Aufgabenliste. Es öffnet sich dabei das Fenster des **Aufgaben-Editors**, dessen Beschreibung Sie unten finden.
4. Sobald Sie mit der Bearbeitung des Zeitplans fertig sind, klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Wenn bei der Bearbeitung ein leerer Zeitplan (ohne Aufgaben) erstellt wird, werden Sie vom **Verwaltungscenter** aufgefordert, entweder einen von den Gruppen vererbten Zeitplan oder den leeren Zeitplan zu verwenden. Der leere Zeitplan muss dann verwendet werden, wenn Sie einen von den Gruppen vererbten Zeitplan überschreiben wollen.

Aufgaben-Editor

Im Aufgabeneditor können Sie Einstellungen für die folgenden Zwecke festlegen:

1. Erstellung einer neuen Aufgabe.

   Klicken Sie dafür auf der Symbolleiste auf **Aufgabe erstellen**.

2. Bearbeitung einer bestehenden Aufgabe.

Klicken Sie dafür in der Aufgabenliste auf den Namen der gewünschten Aufgabe.

Das Fenster zur Bearbeitung der Aufgabenparameter wird angezeigt. Die Einstellungen bei der Bearbeitung einer bestehenden Aufgabe entsprechen denen bei der Erstellung einer neuen Aufgabe.

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

So bearbeiten Sie die Parameter einer Aufgabe

1. Auf der Registerkarte **Allgemein** werden die folgenden Parameter konfiguriert:
   - Im Feld **Name** wird der Name der Aufgabe festgelegt, unter dem sie im Zeitplan angezeigt wird.
   - Um die Aufgabe ausführen zu lassen, aktivieren Sie das Kontrollkästchen **Ausführung zulassen**. Beim deaktivierten Kontrollkästchen wird die Aufgabe in der Liste zwar angezeigt, doch nicht ausgeführt.

   Alterativ können Sie dafür die Option **Status** verwenden, die sich im Hauptfenster des Zeitplans auf der Symbolleiste befindet.

   - Das aktivierte Kontrollkästchen **Kritische Aufgabe** erzwingt die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Agents**, falls die geplante Ausführung versäumt wurde (**Dr.Web Agent** ist zum Zeitpunkt der Aufgabenausführung deaktiviert). Wenn die Aufgabe innerhalb eines Zeitraums mehrmals nicht ausgeführt wurde, wird sie beim Start des **Dr.Web Agents** nur einmal ausgeführt.

   Alternativ können Sie dafür die Option **Schweregrad** verwenden, die sich im Hauptfenster des Zeitplans auf der Symbolleiste befindet.

   Wenn mehrere Scanaufgaben beim Start der Workstation ausgeführt werden sollen, wird nur eine von ihnen, und zwar die erste in der Reihe, ausgeführt.

   Wenn beispielsweise die Aufgabe **Daily scan** geplant wurde und dabei die kritische Aufgabe zum Scannen durch **Agent Scanner** versäumt wurde, wird eben die Aufgabe **Daily scan** ausgeführt. Die verschobene kritische Aufgabe zum Scannen kann dabei nicht durchgeführt werden.

2. Wählen Sie auf der Registerkarte **Aktion** in der Dropdown-Liste **Aktion** einen Aufgabentyp aus und legen Sie die erforderlichen Parameter fest.

Tabelle 6-3: Typen und Parameter der Aufgaben

Aufgabentyp	Parameter und ihre Beschreibung
In die Protokolldatei eintragen	**Zeile** – Text der Meldung, die in die Protokolldatei geschrieben werden soll.
Programm starten	Legen Sie die folgenden Parameter fest: ◆ Geben Sie im Feld **Pfad** den vollständigen Namen (mit der Pfadangabe) der ausführbaren Datei des Programms an, das gestartet werden soll. ◆ Geben Sie im Feld **Argumente** Befehlszeilenparameter für das auszuführende Programm an. ◆ Aktivieren Sie das Kontrollkästchen **Synchron ausführen**, damit das Programm beendet wird, bevor die Ausführung anderer Aufgaben des Typs **Programm starten** beginnt. Wenn das Kontrollkästchen **Synchron ausführen** deaktiviert ist, startet der **Agent** das Programm und protokolliert dabei nur seinen Start. Wenn das Kontrollkästchen **Synchron ausführen** aktiviert ist, protokoliert der **Agent** den Start des Programms, seinen Rückgabecode und seine Endzeit.

Aufgabentyp	Parameter und ihre Beschreibung
Dr.Web Scanner. Schnell **Dr.Web Scanner. Benutzerdefiniert** **Dr.Web Scanner. Vollständig**	Scan-Einstellungen werden unter Workstation scannen detailliert beschrieben.

Der **Scanner** kann nur Workstations unter Windows, UNIX-artigen Betriebssystemen und Mac OS X remote scannen.

3. Auf der Registerkarte **Zeit**:
   - Wählen Sie in der Dropdown-Liste **Periode** einen Startmodus für die Aufgabe und geben Sie an, wie häufig die Aufgabe wiederholt werden soll.

Tabelle 6-4: Startmodi und ihre Parameter

Startmodus	Parameter und ihre Beschreibung
Anfänglich	Die Aufgabe wird beim Start des **Agents** ausgeführt. Für den Start sind keine zusätzlichen Parameter erforderlich.
In N Minuten nach Anfangsaufgabe	Wählen Sie in der Dropdown-Liste **Anfangsaufgabe** die Aufgabe, die als Referenz für die Ausführungszeit der aktuellen Aufgabe dienen soll. Geben Sie im Feld **Minute** die Zeit in Minuten an bzw. wählen Sie diese in der Liste aus, die nach der Ausführung der Anfangsaufgabe vergehen muss, damit die Ausführung der zu bearbeitenden Aufgabe beginnt.
Täglich	Geben Sie die Uhrzeit an, zu der die Aufgabe täglich ausgeführt werden soll.
Monatlich	Geben Sie das Datum und die Uhrzeit an, an dem die Aufgabe monatlich ausgeführt werden soll.
Wöchentlich	Geben Sie den Tag und die Uhrzeit an, an dem die Aufgabe wöchentlich ausgeführt werden soll.
Stündlich	Geben Sie eine Zahl von 0 bis 59 ein: Die Aufgabe wird stündlich zur eingegebenen Minute gestartet.
Alle N Minuten	Geben Sie den Wert **N** ein, um ein Intervall zwischen Aufgaben festzulegen. Wenn der Wert **N** 60 oder mehr beträgt, wird die Aufgabe alle **N** Minuten ausgeführt. Wenn der Wert **N** weniger als 60 beträgt, wird die Aufgabe zu jeder Minute der Stunde, die durch **N** teilbar ist, gestartet.

   - Aktivieren Sie das Kontrollkästchen **Nach der ersten Ausführung verbieten**, damit die Aufgabe zum festgelegten Zeitpunkt einmalig ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe mit der angegebenen Häufigkeit ausgeführt.

   Damit die bereits ausgeführte einmalige Aufgabe erneut ausgeführt wird, klicken Sie auf der Symbolleiste des Zeitplan-Bereichs auf **Wiederholt planen**.

4. Sobald Sie mit der Bearbeitung der Aufgabenparameter fertig sind, klicken Sie auf **Speichern**, um die vorgenommenen Änderungen zu übernehmen (falls Sie eine bereits bestehende Aufgabe bearbeitet haben) bzw. um eine neue Aufgabe mit den festgelegten Parametern zu erstellen (falls Sie eine neue Aufgabe erstellt haben).

6.3.3. Auswahl der zu installierenden Komponenten des Antivirenpakets

So ändern Sie die Liste der zu installierenden Komponenten des Antivirenpakets:

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste eine Workstation oder Gruppe aus. Wählen Sie im geöffneten Verwaltungsmenü den Punkt **Installierte Komponenten**.
2. Wählen Sie in der Dropdown-Liste eine der folgenden Varianten:
   - **Muss installiert werden**. Diese Option gibt an, dass die Komponente auf der Workstation unbedingt installiert werden soll. Bei der Erstellung einer neuen Workstation wird die Komponente zwangsläufig zum zu installierenden Antivirenpaket hinzugefügt. Wenn die Option **Muss installiert werden** für eine bereits vorhandene Workstation aktiviert ist, wird die jeweilige Komponente zum bereits installierten Antivirenpaket hinzugefügt.
   - **Kann installiert werden**. Diese Option gibt an, dass die Komponente eventuell installiert werden kann. Der Benutzer entscheidet selbst, ob die Komponente mit dem **Agent** mitinstalliert werden soll.
   - **Kann nicht installiert werden**. Diese Option verbietet die Installation der Komponente auf der Workstation. Bei der Erstellung einer neuen Workstation wird die Komponente nicht installiert. Wenn die Option **Kann nicht installiert werden** für eine bereits vorhandene Workstation aktiviert ist, wird die jeweilige Komponente des installierten Antivirenpakets entfernt.

   In der Tabelle 6-5 wird angegeben, ob eine Komponente je nach Einstellungen, die vom Benutzer festgelegt wurden, und Einstellungen, die vom Administrator auf dem **Server** festgelegt wurden, auf der Workstation installiert wird (+).

Tabelle 6-5.

Benutzerparameter	Auf dem Server festgelegt		
	Muss	Kann	Kann nicht
Installieren	+	+	
Nicht installieren	+		

3. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern und den Umfang des Antivirenpakets auf der Workstation entsprechend zu ändern.

Die Komponente **Dr.Web Antispam** kann nicht installiert werden, wenn mindestens eines der folgenden Produkte nicht installiert ist:

- **SpIDer Mail**,
- **Dr.Web für Microsoft Outlook**.

6.4. Antivirenkomponenten konfigurieren

So konfigurieren Sie Antivirenkomponenten auf einer Workstation

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
3. Wählen Sie im geöffneten Verwaltungsmenü im Bereich **Konfiguration** des jeweiligen Betriebssystems der Workstation die gewünschte Komponente.
4. Das Fenster mit den Einstellungen der Komponente wird angezeigt.

Die Liste der Einstellungen von Antivirenkomponenten und Empfehlungen zu ihrer Konfiguration finden Sie im **Benutzerhandbuch** für das jeweilige Betriebssystem.

Allerdings können einige Einstellungen im **Verwaltungscenter** und auf Workstations nicht ganz identisch sein.

In diesem Handbuch finden Sie Einstellungen vom **Dr.Web Agent für Windows** (es handelt sich um erweiterte Einstellungen des **Agents**, die für Benutzer von Workstations verfügbar sind), sowie Einstellungen der Antivirenkomponenten, die für Benutzer nicht verfügbar sind.

Achten Sie beim Einrichten der Antivirenkomponenten unter Windows auf folgende Besonderheiten der Protokollierung:

- Die Protokollierungseinstellungen werden im **Verwaltungscenter** individuell für jede Komponente in den Bereichen **Protokoll** festgelegt. Auf der Workstation werden diese Einstellungen hingegen in einem Bereich, und zwar**Erweitert** festgelegt.
- Bei der aktivierten Option **Detailliertes Protokoll führen** wird die Komponente im Debug-Modus umfassend protokolliert. Einschränkung für die Größe der Protokolldatei werden dabei außer Kraft gesetzt. Hierdurch kann es zum Anwachsen der Protokolldatei und zu Leistungsproblemen kommen. Beachten Sie dabei, dass die Rotation der Protokolldatei nicht durchgeführt wird (gilt für jedes Protokollierungsmodus).
  Der Debug-Protokollierungsmodus beeinträchtigt die Leistung des Antivirenprogramms und des Betriebssystems. Verwenden Sie diesen Modus nur dann, wenn Sie Probleme in Komponenten vermuten und dazu vom technischen Support aufgefordert werden. Sie sollten diesen Modus nur für kurze Zeit aktivieren.

Die Benutzeroberfläche des **Verwaltungscenters** unterscheidet sich leicht von der Benutzeroberfläche der jeweiligen Antivirenkomponenten der Workstation:

- Verwenden Sie zur Konfiguration einzelner Einstellungen die entsprechenden Schaltflächen rechts von ihnen:

  Anfangswert wiederherstellen. Diese Option gibt an, dass der ursprüngliche Wert der Einstellung wiederhergestellt werden soll.

  Defaultwert wiederherstellen. Diese Option gibt an, dass der Standardwert der Einstellung wiederhergestellt werden soll.
- Verwenden Sie zur Konfiguration der gesamten Einstellungen die entsprechenden Schaltflächen auf der Symbolleiste:

  Alle Parameter mit den ursprünglichen Werten wiederherstellen. Diese Option gibt an, dass die ursprünglichen (zuletzt gespeicherten) Werte aller Einstellungen des Bereichs wiederhergestellt werden sollen.

  Defaultparameter wiederherstellen. Diese Option gibt an, dass die Standardwerte aller Einstellungen des Bereichs wiederhergestellt werden sollen.

  Diese Einstellungen auf ein anderes Objekt verbreiten. Diese Option gibt an, dass die Einstellungen dieses Bereichs in die Einstellungen einer anderen Workstation, Gruppe oder einiger Gruppen und Workstations kopiert werden sollen.

Vererben von Einstellungen der primären Gruppe setzen. Diese Option gibt an, dass alle individuellen Einstellungen der Workstations durch die jeweiligen Einstellungen der primären Gruppe ersetzt werden sollen.

Einstellungen der primären Gruppe kopieren und diese als persönliche Einstellungen verwenden. Diese Option gibt an, dass die Einstellungen des Bereichs aus der primären Gruppe kopiert werden und auf den ausgewählten Workstations verwendet werden sollen. Die Vererbung findet dabei nicht statt, und die Einstellungen der Workstation gelten als individuell.

Einstellungen aus diesem Bereich in die Datei exportieren. Diese Option gibt an, dass alle Einstellungen des Bereichs in eine Datei gespeichert werden sollen.

Einstellungen aus der Datei in diesen Bereich importieren. Diese Option gibt an, dass alle Einstellungen des Bereichs durch die in einer speziellen Datei enthaltenen Einstellungen ersetzt werden sollen.

5. Sobald Sie alle erforderlichen Änderungen an den Einstellungen über das **Verwaltungscenter** vorgenommen haben, klicken Sie zur Übernahme der Änderungen auf **Speichern**. Die neuen Einstellungen werden an die Workstations übertragen. Wenn eine bzw. mehrere Workstations bei der Konfiguration nicht erreichbar waren, werden die Einstellungen an sie erst dann übertragen, sobald eine Verbindung mit dem **Server** erneut hergestellt wird.

6.4.1. Komponenten

Je nach Betriebssystem können die folgenden Komponenten installiert werden:

Workstations unter Microsoft® Windows®

Dr.Web Scanner, Dr.Web Agent Scanner

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang (auch mit der Suche nach Rootkits) kann auch über das **Verwaltungscenter** remote ausgelöst werden.

SpIDer Guard

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

SpIDer Mail

Scannen aller eingehenden und ausgehenden E-Mails, die durch einen E-Mail-Client übertragen werden.

Dabei kann auch ein Spam-Filter verwendet werden (sofern Ihre Lizenz diese Funktion erlaubt).

SpIDer Gate

Überprüfung aller HTTP-Zugriffe auf Webseiten. Neutralisieren eventueller Bedrohungen im HTTP-Datenverkehr (z. B. in gesendeten oder empfangenen Dateien) sowie Sperren der Zugriffe auf verdächtige oder unerwünschte Ressourcen.

Office Control

Verwalten des Zugriffs auf lokale Ressourcen bzw. Netzwerkressourcen sowie Webseiten. Diese Funktion sorgt für die Integrität wichtiger Dateien, schützt sie vor dem unbeabsichtigten Ändern oder Infizieren durch Viren und verweigert Mitarbeitern den Zugriff auf unerwünschte Inhalte.

Firewall

Diese Komponente schützt Rechner vor dem unbefugten Zugriff von außen und verhindert den Verlust wichtiger Daten über das Internet. Diese Komponente überwacht Internetverbindungen und Datenübertragungen über das Internet und sperrt verdächtige Verbindungen auf der Paket- und Anwendungsebene.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Selbstschutz

Diese Komponente schützt die Dateien und Verzeichnisse von **Dr.Web Enterprise Security Suite** vor dem unbefugten oder unbeabsichtigten Löschen oder Ändern durch Benutzer bzw. bösartige Programme. Beim aktivierten Selbstschutz können nur **Dr.Web** Prozesse auf die Dateien und Verzeichnisse von **Dr.Web Enterprise Security Suite** zugreifen.

Präventivschutz (Einstellungen sind in den Einstellungen des Dr.Web Agents enthalten)

Diese Komponente sorgt für eine frühzeitige Erkennung eventueller Bedrohungen. Dabei werden Zugriffe auf kritische Objekte des Betriebssystems, Treiberladung, automatisch gestartete Programme, laufende Systemdienste und Prozesse überwacht und beim Virenfund gesperrt.

Workstations unter UNIX®

Dr.Web Scanner, Dr.Web Agent Scanner

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote ausgelöst werden.

SpIDer Guard

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

SpIDer Gate

Überprüfung aller HTTP-Zugriffe auf Webseiten. Neutralisieren eventueller Bedrohungen im HTTP-Datenverkehr (z. B. in gesendeten oder empfangenen Dateien) sowie Sperren der Zugriffe auf verdächtige oder unerwünschte Ressourcen.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Andere Komponenten, deren Einstellungen im **Verwaltungscenter** für Workstations unter UNIX-artigen Betriebssystemen angegeben sind, sind optional und dienen zur internen Konfiguration der Antivirensoftware.

Workstations unter Mac OS® X

Dr.Web Scanner, Dr.Web Agent Scanner

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote ausgelöst werden.

SpIDer Guard

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Mobile Endgeräte unter Android OS

Dr.Web Scanner, Dr.Web Agent Scanner

Mobile Endgeräte werden auf Anforderung des Benutzers oder zeitgesteuert gescannt. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote gestartet werden.

SpIDer Guard

Permanentes Echtzeit-Scannen des Dateisystems. Dabei werden auch alle Dateien gescannt, die im Speicher des mobilen Endgeräts abgespeichert werden.

Anruf- und SMS-Filter

Bei der Anruf- und SMS-Filterung werden alle unerwünschten SMS-Nachrichten und Anrufe blockiert, wie z. B. SMS-Werbung oder SMS-Nachrichten und Anrufe von unbekannten Telefonnummern und Kontakten.

Diebstahlschutz

Mit dieser Technologie können Sie Ihre verlorenen bzw. gestohlenen mobilen Endgeräte schnell lokalisieren und sperren.

Cloud Checker

Ein intelligenter URL-Filter schützt Nutzer der mobilen Endgeräte vor unerwünschten Internet-Ressourcen.

Firewall (die Komponente kann nur auf einem mobilen Endgerät eingestellt werden)

Diese Komponente schützt Ihr mobiles Endgerät vor dem unbefugten Zugriff von außen und verhindert den Verlust wichtiger Daten über das Netzwerk. Diese Komponente überwacht Internetverbindungen und Datenübertragungen über das Internet und sperrt verdächtige Verbindungen auf der Paket- und Anwendungsebene.

Sicherheitsprüfer (die Komponente kann nur auf dem mobilen Endgerät eingestellt werden)

Mit diesem Feature können Sie Ihr mobiles Endgerät auf Sicherheitslücken oder andere sicherheitsrelevante Probleme überprüfen und sie bei Bedarf rechtzeitig beheben.

Anwendungsfilter

Diese Komponente verhindert den Start der Anwendungen, die in der Liste vertrauter Anwendungen des mobilen Endgeräts nicht eingetragen sind.

Server unter Novell® NetWare®

Dr.Web Scanner

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers.

SplDer Guard

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

6.4.2. Dr.Web Agent für Windows® konfigurieren

So ändern Sie die Einstellungen des Dr.Web Agents auf einer Workstation unter Windows

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
3. Wählen Sie im Verwaltungsmenü den Punkt**Konfiguration** > **Windows** > **Dr.Web Agent**.
4. Das Fenster mit den Einstellungen des **Agents** wird angezeigt.

Wenn einige Einstellungen (beispielsweise Verschlüsselungs- und Komprimierungsmodus oder Verschlüsselungsschlüssel) aufgrund der vorgenommenen Änderungen nicht mehr mit den entsprechenden Einstellungen des **Servers** übereinstimmen, kann keine Kommunikation zwischen dem **Agent** und **Server** hergestellt werden.

5. Wenn Sie die Einstellungen des **Agents** über das **Verwaltungscenter** geändert haben, klicken Sie zur Übernahme der Änderungen auf **Speichern**.

6.4.2.1. Allgemein

Auf der Registerkarte **Allgemein** können Sie die folgenden Einstellungen des **Agents** konfigurieren:

- Geben Sie im Feld **Startverzögerung des Aufgabenplaners (Min.)** ein Zeitintervall zwischen dem Start des Betriebssystems und der Ausführung der Aufgabe zum Scan beim Start an, falls diese Aufgabe im Aufgabenzeitplan des **Agents** geplant wurde. Der Standardwert beträgt 1 Minute. Wenn Sie 0 angeben, wird die Aufgabe unverzüglich nach dem Start des Betriebssystems ausgeführt.

- Geben Sie im Feld **Zeitintervall für das Versenden der Statistiken (Min.)** das Zeitintervall in Minuten an, in dem der **Agent** alle durch die Komponenten **SpIDer Guard**, **SpIDer Mail** und **SpIDer Gate** erfassten Statistiken an den **Server** versenden soll. Geben Sie 0 an, um keine Statistiken zu versenden.
- Wählen Sie in der Dropdown-Liste **Sprache** die gewünschte Sprache der Benutzeroberfläche des **Agents** und der Komponenten vom **Dr.Web Antivirus** auf der Workstation bzw. Gruppe von Workstations.
- Aktivieren Sie das Kontrollkästchen **Microsoft Network Access Protection aktivieren**, um den Status der Workstation mithilfe der Technologie *Microsoft® Network Access Protection* zu überwachen. Dadurch wird der *Systemintegritäts-Agent* (System Health Agent - SHA) aktiviert, der auf der Workstation zusammen mit der Software des **Dr.Web Agents** installiert wird (Weitere Informationen finden Sie unter NAP Validator).
- Aktivieren Sie das Kontrollkästchen **Remotesteuerung der Quarantäne zulassen**, um die Quarantäne der Workstations vom **Server** aus remote zu verwalten.

Die Option **Remotesteuerung der Quarantäne zulassen** ist nur dann auswählbar, falls im Bereich **Administrierung** → **Dr.Web Server-Konfiguration** → auf der Registerkarte **Statistik** die Option **Status der Quarantäne** aktiviert ist.

- Aktivieren Sie das Kontrollkästchen **Informationen zu Stationen sammeln**, um Informationen zur auf der Workstation installierten Software und Hardware zu sammeln. Falls das Kontrollkästchen aktiviert ist, wählen Sie in der Dropdown-Liste **Zeitabstand für das Sammeln von Informationen über Stationen (Min.)** das Zeitintervall in Minuten aus, in dem der **Agent** die aktuellen Informationen zur Software und Hardware der Workstation an den **Server** senden soll.
- Aktivieren Sie das Kontrollkästchen **Zeit synchronisieren**, um die Systemzeit des Rechners, auf dem der **Agent** installiert ist, mit der Zeit des Rechners, auf dem der **Dr.Web Server** installiert ist, zu synchronisieren.
- Aktivieren Sie das Kontrollkästchen **Ändern des Systemdatums bzw. der Systemzeit verbieten**, damit die Systemzeit automatisch oder manuell nicht geändert werden kann. Diese Option hat keinen Einfluss auf die Zeitsynchronisierung mit dem **Dr.Web Server** (diese wird durch Aktivieren des Kontrollkästchens **Zeit synchronisieren** ausgeführt).
- Aktivieren Sie das Kontrollkästchen **Emulation von Benutzer-Aktionen sperren**, um keine Änderungen an **Dr.Web** zuzulassen. Diese Option gilt nicht für Änderungen, die vom Benutzer manuell vorgenommen werden.
- Aktivieren Sie das Kontrollkästchen **Cloud Services aktivieren**, um die Workstation mit den Cloud Services von **Doctor Web** verbinden zu lassen. Dadurch überprüfen die auf der Workstation laufenden Antivirenkomponenten Daten auf Bedrohungen anhand der aktuellsten Informationen, die von den Servern von **Doctor Web** in Echtzeit gesendet werden. An die Server von **Doctor Web** werden dabei Statistiken zu den auf der Workstation laufenden **Dr.Web** Komponenten automatisch gesendet.

6.4.2.2. Netzwerk

Auf der Registerkarte **Netzwerk** werden die Einstellungen für die Kommunikation mit dem **Server** konfiguriert:

- Im Feld **Öffentlicher Schlüssel** wird der auf der Workstation abgelegte öffentliche Verschlüsselungsschlüssel des **Dr.Web Servers** (`drwcsd.pub`) angegeben. Um eine Schlüsseldatei auszuwählen, klicken Sie auf .

  Auf der Workstation können gleichzeitig mehrere öffentliche Schlüssel gespeichert werden. Das ist der Fall beispielsweise beim Ersetzen der Verschlüsselungsschlüssel oder beim Wechsel von einem **Server** zum anderen. Schlüssel müssen dabei eindeutig sein: Sie können daher zwei identische öffentliche Schlüssel nicht angeben.

Um einen weiteren öffentlichen Schlüssel hinzuzufügen, klicken Sie auf und wählen Sie die gewünschte Schlüsseldatei.

Um einen vorhandenen Schlüssel zu entfernen, klicken Sie auf .

Bei der deaktivierten Option **Betrieb ohne öffentlichen Schlüssel erlauben** kann der letzte öffentliche Schlüssel nicht entfernt werden.

- Aktivieren Sie das Kontrollkästchen **Betrieb ohne öffentlichen Schlüssel erlauben**, damit **Agents**, die keinen öffentlichen oder einen beschädigten Schlüssel (`drwcsd.pub`) besitzen, eine Verbindung herstellen können.
- Aktivieren Sie das Kontrollkästchen **Betrieb mit dem ungültigen öffentlichen Schlüssel erlauben**, damit **Agents**, die einen falschen öffentlichen Schlüssel (`drwcsd.pub`) besitzen, eine Verbindung herstellen können.
- Geben Sie im Feld **Server** die Adresse des **Dr.Web Servers** an. Sie können aber dieses Feld leer lassen. In diesem Fall verwendet der **Agent** als Adresse des **Dr.Web Servers** die Angaben in den jeweiligen Einstellung auf dem lokalen Rechner des Benutzers (die Adresse des **Servers**, von dem aus die Installation initiiert wurde).

  Sie können sowohl eine Adresse des **Servers** als auch mehrere Adressen verschiedener **Server-Adresse** angeben. Um eine weitere Adresse des **Servers** hinzuzufügen, klicken Sie auf und geben ins Feld die gewünschte Adresse ein. Das Format von Netzwerkadressen des **Servers** wird im Dokument **Anhänge** im Abschnitt Anhang E. Spezifikation der Netzwerkadresse detailliert beschrieben.

  Beispiel einer Adresse des **Servers**:

  ```
  tcp/10.4.0.18:2193
  tcp/10.4.0.19
  10.4.0.20
  ```

Wenn Sie einen falschen/ungültigen Wert für den Parameter **Server** festlegen, beendet der **Agent** die Verbindung mit dem **Server** und kann dann keine Verbindung mit ihm erneut herstellen. In diesem Fall müssen Sie die Adresse des **Servers** direkt auf der Workstation angeben.

- Geben Sie im Feld **Wiederholungen bei der Suche** die Anzahl der Wiederholungsversuche beim Suchen nach dem **Dr.Web Server** an, falls Sie den Multicast-Modus verwenden.
- Geben Sie im Feld **Timeout der Suche (Sek.)** die Anzahl der Sekunden zwischen den Suchvorgängen nach dem **Dr.Web Server** an, falls Sie den Multicast-Modus verwenden.
- Konfigurieren Sie in den Feldern **Komprimierungsmodus** und **Verschlüsselungsmodus** die Komprimierung und Verschlüsselung des Netzwerkdatenverkehrs (mehr dazu finden Sie unter Datenverkehr verschlüsseln und komprimieren).
- Gegen Sie im Feld **Parameter zum Abhören des Netzwerks** einen UDP-Port an, den das **Verwaltungscenter** für die Suche nach aktiven **Dr.Web Agents** verwenden soll. Damit an keinen Ports gelauscht wird, geben Sie hier **NONE** ein.

  Der Wert dieses Parameters sollte im Format einer Netzwerkadresse angegeben werden. Die erlaubten Schreibweisen finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen.

  Der Standardwert ist **udp/:2193**, d. h. „alle Schnittstellen, Port 2193".

6.4.2.3. Mobilität

Auf der Registerkarte **Mobilität** werden die Einstellungen für den *mobilen Modus* des **Agents** konfiguriert:

- Geben Sie im Feld **Aktualisierungsfrequenz** das Zeitintervall zwischen den Aktualisierungen der Antivirensoftware an.
- Aktiveren Sie das Kontrollkästchen **Proxy-Server nutzen**, um einen HTTP-Proxy-Server für die Aktualisierung über das Internet zu verwenden. Um den gewünschten Proxy-Server einzustellen, füllen Sie die hier verfügbaren Felder entsprechend aus.

6.4.2.4. Protokoll

Auf der Registerkarte **Protokoll** werden die Parameter für die Protokollierung von Aktivitäten des **Agents** und einiger Komponenten des **Dr.Web Antivirus** festgelegt:

- Der Parameter **Detailstufe für das Agent-Protokoll** bestimmt die Ausführlichkeit der Protokollierung von Aktivitäten des **Agents**.
- Der Parameter **Detailstufe für das Engine-Protokoll** bestimmt die Ausführlichkeit der Protokollierung von Aktivitäten der Scan-Engine (Scanning Engine).
- Der Parameter **Detailtiefe des Update-Protokolls** gibt an, wie ausführlich das Protokoll des **Dr.Web** Updaters sein soll.
- Aktivieren Sie das Kontrollkästchen **Speicherauszüge bei Scan-Fehlern erstellen**, damit Speicherauszüge bei Scan-Fehlern erstellt werden. Es empfiehlt sich, diese Option immer aktiviert zu halten, um eventuelle Fehler in **Dr.Web** genau zu diagnostizieren und rechtzeitig zu beheben.

6.4.2.5. Interface

Auf der Registerkarte **Interface** können Sie die Oberfläche des **Dr.Web Agents** individuell anpassen:

- Aktivieren Sie das Kontrollkästchen **Icon in der Taskleiste anzeigen**, um das Symbol des **Agents** auf der Taskleiste anzeigen zu lassen. Wenn das Symbol deaktiviert ist, kann der Benutzer die Einstellungen des **Agents** und des Antivirenpakets weder ansehen noch bearbeiten.
- Aktivieren Sie das Kontrollkästchen **Neustart-Anforderung anzeigen** , um zu Neustart der Workstation aufgefordert zu werden. Beim deaktivierten Kontrollkästchen wird auf der Workstation keine Neustartaufforderung angezeigt, und erfolgt kein automatischer Neustart. In den Statistiken der Workstation, die an das **Verwaltungscenter** versendet werden, erscheint der entsprechende Hinweis. Die Neustartaufforderung wird in der TabelleStatus angezeigt. Der Administrator kann dann die Workstation über das **Verwaltungscenter** (s. den Abschnitt Antivirus-Netzwerk) manuell neu starten.

Wählen Sie die Ereignisse aus, über die Benutzer benachrichtigt werden sollen. Aktivieren Sie dafür die entsprechenden Kontrollkästchen:

- **Kritische Benachrichtigungen**. Diese Option gibt an, dass nur kritische Benachrichtigungen angezeigt werden sollen. Darunter fallen:
  - Hinweis auf Fehler bei der Aktualisierung der Antivirensoftware oder einer Antivirenkomponente.
  - Hinweis auf den anstehenden Neustart des Rechners nach einem Update.

  Diese Berechtigungen werden nur für Benutzer mit Administratorrechten angezeigt.
- **Benachrichtigungen über Bedrohungen**. Diese Option gibt an, dass nur Benachrichtigungen über Bedrohungen angezeigt werden sollen. Diese Benachrichtigung wird dann ausgegeben, wenn eine der Komponenten von Antivirensoftware einen Virus (Viren) erkennt.
- **Wichtige Benachrichtigungen**. Diese Option gibt an, dass nur wichtige Benachrichtigungen angezeigt werden sollen. Darunter fallen die folgenden Hinweise:

- Hinweis auf Fehler beim Start einer der Antivirenkomponenten.
- Hinweis auf Fehler beim Update der Antivirensoftware oder einer Antivirenkomponente. Diese Benachrichtigung wird sofort nach einem fehlgeschlagenen Update angezeigt.
- Hinweis auf den anstehenden Neustart des Rechners. Diese Benachrichtigung wird sofort nach einem erfolgreichen Update angezeigt.
- Hinweis auf das Abwarten der Neustartaufforderung am Ende der Installation von Komponenten.

◆ **Geringfügige Benachrichtigungen**. Diese Option gibt an, dass nur geringfügige Benachrichtigungen angezeigt werden sollen. Darunter fallen die folgenden Hinweise:

- Hinweis auf den Start eines ferngesteuerten Scanvorgangs.
- Hinweis auf den Abschluss eines ferngesteuerten Scanvorgangs.
- Hinweis auf den Start der Aktualisierung der Antivirensoftware oder einer Antivirenkomponente.
- Hinweis auf die erfolgreiche Aktualisierung der Antivirensoftware oder einer Antivirenkomponente (ohne Neustart).

Wenn Sie wollen, dass Benutzer alle obigen Benachrichtigungen erhalten können, aktivieren Sie alle Kontrollkästchen. Anderenfalls werden nur Benachrichtigungen der ausgewählten Gruppe ausgegeben.

Der Benutzer kann die Anzeige von Benachrichtigungen individuell anpassen. Die Anzeige der **kritischen Benachrichtigungen** kann dabei nur vom Administrator geändert werden.

Die Anzeige von Benachrichtigungen kann über das **Verwaltungscenter** solange angepasst werden, bis sie vom Benutzer der Workstation zum ersten Mal geändert wird. Einmal durch den Benutzer angepasst, kann die Anzeige von Benachrichtigungen nur über das Kontextmenü des **Agents** erneut geändert werden.

Im Unterbereich **Erweitert** können Sie die folgenden Einstellungen konfigurieren:

◆ Aktivieren Sie das Kontrollkästchen **Benachrichtigung nicht im Vollbildmodus anzeigen**, damit keine Popup-Benachrichtigungen angezeigt werden, während ein Programm im Vollbildmodus ausgeführt wird.

◆ Aktivieren Sie das Kontrollkästchen **Benachrichtigungen der Firewall im separaten Fenster im Vollbildmodus anzeigen**, damit Benachrichtigungen der **Dr.Web Firewall** in einem separaten Fenster angezeigt werden. Es empfiehlt sich, diese Option zu aktivieren, damit die Netzwerkverbindungen, die von im Vollbildmodus laufenden Anwendungen verwendet werden, nicht blockiert werden. Anderenfalls können Sie diese Verbindungen nicht zulassen, wenn die **Dr.Web Firewall** Sie darüber informiert.

6.4.2.6. Präventivschutz

Auf der Registerkarte **Präventiver Schutz** im Bereich **Ebene der Sperrung der verdächtigen Aktivitäten** können Sie die Reaktion von **Dr.Web** auf verdächtige Aktivitäten fremder Anwendungen konfigurieren. Mit dieser Funktion schützen Sie auch Benutzerdaten vor unerwünschten Änderungen.

Wählen Sie eine der möglichen Schutzebenen:

◆ **Vergesslich**. Diese Option bietet die maximale Schutzebene, bei der Zugriffe auf alle kritischen Windows-Objekte überwacht werden.

Dieser Schutzmodus kann in einigen Fällen zu Kompatibilitätsproblemen mit Drittanbieterprogrammen, welche die geschützten Verzeichnisse der Registrierungsdatenbank verwenden, führen.

◆ **Medium**. Diese Schutzebene kann ausgewählt werden, wenn der Rechner einem hohen Infizierungsrisiko ausgesetzt ist. In diesem Modus werden Zugriffe auf diejenigen kritischen Objekte unterbunden, die bösartige Programme ausnutzen können.

- **Optimal**. Auf dieser Schutzebene wird die automatische Änderung von Systemobjekten, deren Modifikation eindeutig auf einen bösartigen Angriff auf das Betriebssystem hinweist, unterbunden.
- **Benutzerdefiniert**. In diesem Modus konfiguriert der Benutzer (Administrator des **Servers**) selbst die in der Tabelle unten aufgeführten Einstellungen für den Präventivschutz.

  Um den Präventivschutz individuell zu konfigurieren, aktivieren Sie für jede Einstellung in der Tabelle eines der drei runden Optionsfelder:

  - **Erlauben**. Jegliche Aktionen mit dem Objekt bzw. des Objekts immer erlauben.
  - **Frage stellen**. Das Dialogfenster anzeigen, in dem der Benutzer aufgefordert wird, die jeweilige Aktion für das Objekt zu erlauben bzw. zu verbieten.
  - **Sperren**. Jegliche Aktionen mit dem Objekt bzw. des Objekts immer verbieten.

  Wenn Sie eine oder mehrere Einstellungen in der Tabelle ändern, wird die im Feld **Ebene der Sperrung der verdächtigen Aktivitäten** vordefinierte Schutzebene durch **Benutzerdefiniert** automatisch ersetzt.

Die Einstellungen des Präventivschutzes ermöglichen Ihnen, die folgenden Objekte zu überwachen:

- **Integrität von laufenden Anwendungen**. Diese Option sorgt für die Überwachung der Prozesse, die in die gestarteten Anwendungen eindringen und dadurch die Sicherheit des Rechners bedrohen können. Die zur Ausnahmeliste von **SpIDer Guard** hinzugefügten Prozesse werden nicht überwacht.
- **Integrität von Benutzerdateien**. Diese Option sorgt für die Überwachung der Prozesse, die Benutzerdateien nach einem bekannten Algorithmus modifizieren und dadurch die Sicherheit des Rechners bedrohen können. Die zur Ausnahmeliste von **SpIDer Guard** hinzugefügten Prozesse werden nicht überwacht. Um Daten der Benutzer vor unbefugten Änderungen zu schützen, sollten Sie die Erstellung der geschützten Kopien von wichtigen Dateien konfigurieren.
- **HOSTS-Datei**. Diese Datei wird vom Betriebssystem für den leichteren Zugang zum Internet verwendet. Änderungen in dieser Datei weisen auf eine eventuelle Manipulation durch einen Virus oder ein bösartiges Programm hin.
- **Laufwerkszugriff auf niedriger Ebene**. Diese Option verweigert Anwendungen direkten Schreibzugriff auf einzelne Sektoren der Festplatte.
- **Treiber herunterladen**. Diese Option verweigert Anwendungen, neue oder unbekannte Treiber herunterzuladen.

Die restlichen Einstellungen sorgen für den Schutz von kritischen Windows-Bereichen und ermöglichen, Verzeichnisse der Registrierungsdatenbank (sowohl im Systemprofil als auch in allen Benutzerprofilen) vor unbefugten Änderungen zu schützen.

Tabelle 6-6: Geschützte Verzeichnisse der Registrierungsdatenbank

Einstellung	Schlüssel der Registrierdatenbank
Image File Execution Options	Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
User Drivers	Software\Microsoft\Windows NT\CurrentVersion\Drivers32 Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Parameter der Winlogon-Benutzeroberfläche	Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Winlogon-Melder	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Autostart der Windows-Benutzeroberfläche	Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib
Verknüpfungen ausführbarer Dateien	Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (Schlüssel) Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (Schlüssel)
Richtlinien für Softwareeinschränkungen (SRP)	Software\Policies\Microsoft\Windows\Safer

Einstellung	Schlüssel der Registrierdatenbank
Internet Explorer Plug-Ins (BHO)	Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Autostart des Programms	Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\RunOnce Software\Microsoft\Windows\CurrentVersion\RunOnceEx Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup Software\Microsoft\Windows\CurrentVersion\RunServices Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
Autostart der Richtlinien	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Abgesicherten Modus konfigurieren	SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Parameter von Session Manager	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
Systemdienste	System\CurrentControlXXX\Services

Wenn bei der Installation wichtiger Microsoft-Updates bzw. bei der Installation und Ausführung von Programmen (darunter auch Defragmentierungsprogrammen) Probleme auftreten, deaktivieren Sie in dieser Gruppe von Einstellungen die entsprechenden Optionen.

6.4.3. SpIDer Mail für Windows® konfigurieren. Anwendungsfilter

Mit dem **Anwendungsfilter** können Sie sämtliche Verbindungen mit E-Mail-Servern manuell abfangen. In diesem Modus wird **SpIDer Mail** als Proxy-Server zwischen E-Mail-Clients und E-Mail-Servern geschaltet, der nur diejenigen Verbindungen überwacht, die in den Einstellungen explizit angegeben sind. Um diesen Modus verwenden zu können, müssen Sie auf den Workstations einige Einstellungen für die Verbindung von E-Mail-Clients ändern.

Die Liste der abzufangenden Verbindungen besteht aus Einträgen, jede von denen eine Übereinstimmung zwischen den Einstellungen von **SpIDer Mail** und dem verwendeten E-Mail-Client festlegt.

Die Liste ist standardmäßig leer. Sie können bei Bedarf gewünschte Einträge hinzufügen.

Abfangen von Verbindungen einstellen

1. Stellen Sie die Liste von E-Mail-Servern zusammen, die Sie überwachen wollen. Weisen Sie diesen Servern beibiege Portnummern zu. Verwenden Sie dabei nur freie Ports, die vom System nicht reserviert sind. Diese Ports werden nachfolgend *SpIDer Mail-Ports* genannt.

SpIDer Mail unterstützt E-Mail-Server, die Protokolle POP3, SMTP, IMAP4 oder NNTP verwenden.

2. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
3. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
4. Wählen Sie im Verwaltungsmenü den Punkt**Konfiguration** > **Windows** > **SpIDer Mail**. Wechseln Sie dann zur Registerkarte **Anwendungsfilter**.
5. Geben Sie im Bereich **Verbindungen von SpIDer Mail konfigurieren** die folgenden Parameter an:
   - **SpIDer Mail Port**– *SpIDer Mail-Port*, die Sie dem E-Mail-Server im Schritt 1 zugewiesen haben.

- **Server** – Domänenname oder IP-Adresse des E-Mail-Servers.
- **Port** – Nummer des Ports, der E-Mail-Server verwendet.

6. Wiederholen Sie bei Bedarf den Schritt 5 für andere Server. Um einen weiteren Server hinzuzufügen, klicken Sie auf .
7. Wenn Sie wollen, dass eine Verbindung nicht mehr abgefangen wird, klicken Sie neben dem gewünschten Server auf .
8. In der Liste **Ausgenommene Anwendungen** können Sie die Anwendungen angeben, die von der Überwachung durch die Komponente **SpIDer Mail** ausgeschlossen werden sollen:
   a) Um eine Anwendung zu Ausnahmen hinzuzufügen, geben Sie den Pfad zur ausführbaren Datei der Komponente an.
   b) Sie können nur eine Anwendung pro Feld angeben. Um ein neues Element hinzuzufügen, klicken Sie auf .
   c) Wenn Sie eine Anwendung aus der Listen entfernen wollen, klicken Sie neben dem gewünschten Anwendung auf .
9. Nachdem alle erforderlichen Einstellungen festgelegt sind, klicken Sie auf **Speichern**, damit die vorgenommenen Äderungen wirksam werden.

Der **Anwendungsfilter** der Komponente **SpIDer Mail** kann nur am **Dr.Web Server** konfiguriert werden. Benutzer von Workstations haben keinen Zugriff auf den Filter.

10. Konfigurieren Sie den E-Mail-Client auf der Workstation so, dass die Komponente **SpIDer Mail** Verbindungen abfangen kann.

E-Mail-Client einstellen

Wenn Sie die Komponente **SpIDer Mail** zum manuellen Abfangen von Verbindungen mit E-Mail-Servern verwenden wollen, müssen Sie die Einstellungen des auf der Workstation instillierten E-Mail-Clients entsprechend anpassen:

1. Geben Sie als Adresse des Posteingangs- und Postausgangsservers den Wert `localhost` an.
2. Geben Sie als Port des E-Mail-Servers den *SpIDer Mail-Port*, den Sie dem E-Mail-Server zugewiesen haben.

In der Regel müssen Sie dafür in den Einstellungen des E-Mail-Servers folgende Werte angegeben:

`localhost:`<*SpIDer_Mail_Port*>

wobei <*SpIDer_Mail_Port*> der Port ist, der Sie dem E-Mail-Server zugewiesen haben.

Beispiel:

Wenn Sie dem E-Mail-Server mit der Adresse `pop.gmail.com` und dem Port `110` den *SpIDer Mail-Port* `7000` zugewiesen haben, müssen Sie in den Einstellungen des E-Mail-Clients als Posteingangsserver `localhost` und als Port `7000` angeben.

6.5. Workstations scannen

Mit der Komponente **Dr.Web Scanner für Windows** können Benutzer ihre Workstations selbständig scannen lassen. Das Programmsymbol zum Starten dieser Komponente wird auf dem Desktop bei der Installation der Antivirensoftware automatisch erstellt. Der **Scanner** kann auch dann verwendet werden, wenn der **Agent** seine regulären Aufgaben nicht funktionsgerecht bewältigen kann, oder Windows im abgesicherten Modus gestartet wurde.

Das Verwaltungscenter bietet Ihnen die folgenden Möglichkeiten:

- Anzeigen aller laufenden Antivirenkomponenten.
- Anhalten einzelner Antivirenkomponenten.
- Einstellen und Starten von Aufgaben zum Scannen.

6.5.1. Gestartete Komponenten anzeigen und abbrechen

So kontrollieren bzw. beenden Sie die gestarteten Komponenten

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe. Wählen Sie im geöffneten Verwaltungsmenü den Punkt **Gestartete Komponenten**.

   Die Liste mit allen zum aktuellen Zeitpunkt laufenden Komponenten, die sowohl vom Administrator manuell über das **Verwaltungscenter** bzw. nach Zeitplan als auch vom Benutzer der Workstation gestartet wurden, wird angezeigt.

2. Um eine Komponente abzubrechen, aktivieren Sie das Kontrollkästchen neben dieser Komponente und klicken Sie danach auf der Symbolleiste die Schaltfläche **Abbrechen** an.

Wenn Sie so vorgehen, werden die laufenden Scanvorgänge abgebrochen, der **Scanner** wird beendet und die gestarteten Wächter werden angehalten.

Beachten Sie: die Wächter **SpIDer Guard**, **SpIDer Mail** und **SpIDer Gate** können über das **Verwaltungscenter** nicht gestartet werden.

6.5.2. Gestartete Komponenten nach Typ abbrechen

Wenn Sie so vorgehen, werden die laufenden Scanvorgänge abgebrochen, der **Scanner** wird beendet und die gestarteten Wächter werden angehalten.

Beachten Sie: die Wächter **SpIDer Guard**, **SpIDer Mail** und **SpIDer Gate** können über das **Verwaltungscenter** nicht gestartet werden.

So beenden Sie alle auf einer Workstation laufenden Komponenten eines bestimmten Typs

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Bereich **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste eine Gruppe oder einzelne Workstations aus.
2. Klicken Sie auf der Symbolleiste des Antivirus-Netzwerks auf **Komponentenverwaltung**. Wählen Sie in der Dropdown-Liste den Punkt **Gestartete Komponenten abbrechen**.
3. Aktivieren Sie im geöffneten Bereich die Kontrollkästchen neben den Komponententypen, die Sie unverzüglich abbrechen wollen:

- **Nach Zeitplan gestarteten Dr.Web Agent Scanner unterbrechen**. Diese Option gibt an, dass der nach dem zentralen Aufgabenzeitplan gestartete und derzeit laufende Scanvorgang durch **Dr.Web Agent Scanner** abgebrochen werden soll.
- **Von dem Administrator gestarteten Dr.Web Agent Scanner unterbrechen**. Diese Option gibt an, dass der vom Administrator über das **Verwaltungscenter** manuell gestartete und derzeit laufende Scanvorgang durch **Dr.Web Agent Scanner** abgebrochen werden soll.
- **Durch Benutzer gestarteten Dr.Web Scanner unterbrechen**. Diese Option gibt an, dass der vom Benutzer der Workstation manuell gestartete und derzeit laufende Scanvorgang durch **Dr.Web Agent Scanner** abgebrochen werden soll.
- **SpIDer Guard, SpIDer Mail, SpIDer Gate, Office-Kontrolle, Firewall und Selbstschutz unterbrechen**. Diese Option gibt an, dass **SpIDer Guard**, **SpIDer Mail**, **SpIDer Gate**, **Firewall** und **Selbstschutz** vorübergehend angehalten werden sollen.

Um alle Typen der abzubrechenden Komponenten auszuwählen, aktivieren Sie das Kontrollkästchen neben der Überschrift des Bereichs **Unterbrechen der gestarteten Komponenten**.

4. Klicken Sie auf **Abbrechen**.

6.5.3. Scanvorgang starten

So lassen Sie Workstations scannen

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
3. Klicken Sie auf der Symbolleiste auf **Scannen**. Wählen Sie in der Liste auf der Symbolleiste einen Scanmodus aus:

Dr.Web Scanner. Schnell. In diesem Modus werden die folgenden Objekte gescannt:

- Arbeitsspeicher
- Startsektoren aller Festplatten
- Autostart-Objekte
- Stammverzeichnis des Startsektors
- Stammverzeichnis des Windows-Laufwerks
- Windows-Systemverzeichnis
- Ordner `Eigene Dateien`
- TEMP-Verzeichnis des Systems
- TEMP-Verzeichnis des Benutzers

Dr.Web Scanner. Vollständig. In diesem Modus werden alle Festplatten und Wechseldatenträger (darunter auch Startsektoren) komplett gescannt.

Dr.Web Scanner. Benutzerdefiniert. Dieser Modus bietet Ihnen die Möglichkeit, einzelne Verzeichnisse und Dateien scannen zu lassen und entsprechende erweiterte Scan-Einstellungen zu konfigurieren.

> Der **Scanner** kann nur aktive Workstations remote scannen, die unter einem der vom **Scanner** unterstützten Betriebssystemen laufen. Diese Betriebssysteme sind Windows, Unix-artige Betriebssysteme und Mac OS X.

4. Nachdem Sie den gewünschten Modus ausgewählt haben, öffnet sich das Fenster mit den Einstellungen des **Scanners**. Sie können diese bei Bedarf individuell anpassen (s. dazu den Abschnitt Scanner konfigurieren).
5. Klicken Sie auf **Auf Viren überprüfen**, um die ausgewählten Workstations scannen zu lassen.

Das Scannen von Workstations über **Dr.Web Agent Scanner**, der remote gestartet wurde, läuft im Hintergrundmodus, sodass der Benutzer der jeweiligen Workstation nicht darüber informiert wird.

6.5.4. Scanner konfigurieren

Über das Verwaltungscenter können Sie die folgenden Scaneinstellungen festlegen:

- Einstellungen des **Dr.Web Scanners**. Dieser **Scanner** wird vom Benutzer der jeweiligen Workstation gestartet und kann nicht über das **Verwaltungscenter** remote gestartet werden. Der Administrator kann aber seine Einstellungen zentral ändern. Die vorgenommenen Änderungen werden dann an die betroffenen Workstations übermittelt und dort übernommen.
- Einstellungen des **Dr.Web Agent Scanners**. Dieser **Scanner** wird remote über das **Verwaltungscenter** gestartet und scannt Verzeichnisse und Dateien genauso wie der **Dr.Web Scanner**. Bei den Einstellungen des **Dr.Web Agent Scanners** handelt es sich um die erweiterten Einstellungen des **Dr.Web Scanners**: Sie werden beim Start eines Scanvorgangs festgelegt.

Einstellungen des Dr.Web Scanners festlegen

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
3. Wählen Sie im geöffneten Verwaltungsmenü unter **Konfiguration** im Unterbereich des benötigten Betriebssystems den Punkt **Scanner**. Das Fenster mit den Einstellungen des **Scanners** wird geöffnet.
4. Legen Sie alle erforderlichen Scaneinstellungen fest. Die Einstellungen des **Dr.Web Scanners** werden im **Benutzerhandbuch** für das jeweilige Betriebssystem detailliert beschrieben.
5. Klicken Sie auf **Speichern**. Die Einstellungen werden im **Verwaltungscenter** gespeichert und an die betroffenen Workstations übertragen.

Einstellungen des Dr.Web Agent Scanners festlegen

Die Einstellungen des **Dr.Web Agent Scanners** werden beim Start eines Scanvorgangs wie unter Scanvorgang starten beschrieben festgelegt.

Gruppen der Einstellungen des **Scanners**, die je nach Scanmodus verfügbar (+) bzw. nicht verfügbar (–) sind, werden in der unten stehenden Tabelle aufgeführt.

Tabelle 6-7: Liste der Gruppen der Einstellungen des Scanners je nach Scanmodus

Scan-Modus	Gruppen von Einstellungen			
	Allgemein	Aktionen	Einschränkungen	Ausnahmen
Dr.Web Scanner. Benutzerdefiniert	+	+	+	+
Dr.Web Scanner. Schnell	–	+	+	–
Dr.Web Scanner. Vollständig	–	+	+	–

Je nach Betriebssystem der Workstation, auf welcher der Scanvorgang remote gestartet wird, sind nur diejenigen Einstellungen des **Scanners** verfügbar, die vom jeweiligen Betriebssystem der Workstation unterstützt werden.

Die Einstellungen, die beim Scannen der Workstations unter UNIX- und Mac OS X-basierten Betriebssystemen nicht unterstützt werden, sind mit dem Zeichen [] gekennzeichnet.

6.5.4.1. Allgemein

Die Einstellungen, die beim Scannen der Workstations unter UNIX- und Mac OS X-basierten Betriebssystemen nicht unterstützt werden, sind mit dem Zeichen [] gekennzeichnet.

Im Bereich **Allgemein** sind die folgenden Scan-Einstellungen verfügbar:

- Aktivieren Sie das Kontrollkästchen **Heuristische Analyse verwenden**, damit der **Scanner** die heuristische Analyse zur Suche nach unbekannten Viren verwenden kann. In diesem Modus können auch Fehlerkennungen vorkommen.
- Aktivieren Sie das Kontrollkästchen **Boot-Sektoren scannen**, damit der **Scanner** Boot-Sektoren überprüft. Gescannt werden sowohl die Boot-Sektoren der logischen Laufwerke als auch der Master Boot Record der physikalischen Laufwerke.
- Aktivieren Sie das Kontrollkästchen **Autostart-Programme scannen**[], damit die beim Start des Betriebssystems automatisch gestarteten Programme überprüft werden.
- Aktivieren Sie das Kontrollkästchen **Symbolischen Links folgen**, um Symbolischen Verknüpfungen beim Scannen zu folgen.
- Aktivieren Sie das Kontrollkästchen **Laufende Programme und Module prüfen**[], um die im Arbeitsspeicher befindlichen Prozesse zu überprüfen.
- Aktivieren Sie das Kontrollkästchen **Auf Rootkits prüfen**[], um die Suche nach versteckten Schadprogrammen zu aktivieren.
- Aktivieren Sie das Kontrollkästchen **Prüfung beim Wechsel zur Batteriespeisung abbrechen**[], um den Scanvorgang beim Wechsel des Rechners in den Akkubetrieb abzubrechen.
- Die Dropdown-Liste **Scanpriorität** bestimmt die Ausnutzung der vorhandenen Systemressourcen.
- Aktivieren Sie das Kontrollkästchen **CPU-Auslastung einschränken**[], um die Nutzung der Systemressourcen beim Scannen einzuschränken. Wählen Sie in der Dropdown-Liste die maximal zulässige Systemauslastung durch den **Scanner** aus. Wenn es keine anderen Aufgaben gibt, werden die CPU-Ressourcen maximal beansprucht.
- In der Dropdown-Liste **Aktionen nach der Prüfung** können Sie festlegen, welche Aktion nach dem Suchlauf automatisch ausgeführt werden soll:
  - **Zurückhalten**. Nach dem Suchlauf werden keine weiteren Aktionen am Rechner des Benutzers durchgeführt.
  - **Station herunterfahren**[]. Der Rechner des Benutzers wird nach dem Suchlauf heruntergefahren. Vor dem Herunterfahren behandelt der **Scanner** alle gefundenen Bedrohungen entsprechend den festgelegten Einstellungen.
  - **Station neu starten**. Der Rechner des Benutzers wird nach dem Suchlauf neu gestartet. Vor dem Neustart behandelt der **Scanner** alle gefundenen Bedrohungen entsprechend den festgelegten Einstellungen.
  - **Station suspendieren**.
  - **Station auf Standby schalten**.
- Aktivieren Sie das Kontrollkästchen **Netzwerkverbindung während der Prüfung deaktivieren**, um den Rechner vom lokalen Netzwerk und Internet beim Scannen zu trennen.
- Aktivieren Sie das Kontrollkästchen **Festplatten scannen**, um Festplattenlaufwerke (HDD u. ä.) zu scannen.
- Aktivieren Sie das Kontrollkästchen **Wechseldatenträger prüfen**, um alle Wechseldatenträger, darunter magnetische Datenträger (Disketten), CDs und DVDs, Flash-Speicher usw., zu scannen.
- Geben Sie im Feld **Zum Scannen ausgewählte Pfade** die zu scannenden Pfade an (das Eingabeverfahren wird unten beschrieben).
  - Um eine neue Zeile der Liste hinzuzufügen, klicken Sie auf und geben Sie in die geöffnete Zeile den gewünschten Pfad ein.

- Um ein Element aus der Liste zu entfernen, klicken Sie auf neben der benötigten Zeile.

Wenn das Kontrollkästchen **Zum Scannen ausgewählte Pfade** aktiviert ist, werden nur die angegebenen Pfade gescannt. Beim deaktivierten Kontrollkästchen werden alle Laufwerke gescannt.

6.5.4.2. Aktionen

Die Einstellungen, die beim Scannen der Workstations unter UNIX- und Mac OS X-basierten Betriebssystemen nicht unterstützt werden, sind mit dem Zeichen [1] gekennzeichnet.

Im Bereich **Aktionen** können Sie festlegen, welche Aktion der **Scanner** ausführen soll, wenn infizierte oder verdächtige Dateien, Schadprogramme sowie infizierte Archive gefunden wurden.

Dr.Web Agent Scanner führt automatisch die für erkannte schädliche Objekte festgelegten Aktionen aus.

Folgende Aktionen können für gefundene schädliche Objekte ausgeführt werden:

- **Desinfizieren** – den ursprünglichen Zustand des Objekts wiederherstellen. Wenn das betroffene Objekt nicht desinfizierbar ist oder die Desinfektion nicht erfolgreich war, wird die für nicht desinfizierbare Objekte festgelegte Aktion ausgeführt.

  Die Ausführung dieser Aktion ist nur für die Objekte möglich, die mit einem bekannten desinfizierbaren Virus infiziert wurden. Ausgenommen sind Trojaner und die in zusammengesetzten Objekten (Archiven, E-Mail-Dateien bzw. Container-Dateien) enthaltenen infizierten Dateien.

- **Entfernen** – infizierte Objekte löschen.
- **In Quarantäne verschieben** – infizierte Objekte in das Verzeichnis der **Quarantäne** der Workstation verschieben.
- **Benachrichtigen** – Benachrichtigung über Virenfund an das **Verwaltungscenter** senden (mehr dazu finden Sie unter Benachrichtigungen konfigurieren).
- **Ignorieren** – keine Aktionen für das betroffene Objekt ausführen und keine Benachrichtigungen senden.

Tabelle 6-8: Aktionen des Scanners bei Fund

Objekt	Aktion				
	Desinfizieren	Entfernen	In Quarantäne verschieben	Benachrichtigen	Ignorieren
Infiziert	+/*	+	+		
Verdächtig		+	+/*		+
Nicht desinfizierbar		+	+/*		
Infizierte Container		+	+/*		
Infizierte Archive		+	+/*		
Infizierte E-Mail-Dateien			+/*		+
Boot-Sektoren	+/*			+	
Adware		+	+/*		+
Dialer		+	+/*		+
Scherzprogramme		+	+/*		+
Riskware		+	+/*		+

Objekt	Aktion				
	Desinfizieren	Entfernen	In Quarantäne verschieben	Benachrichtigen	Ignorieren
Hacktools		+	+/*		+

Symbole

+	Aktion ist erlaubt für diesen Typ von Objekten
+/*	Diese Aktion ist die Standardaktion für diesen Typ von Objekten

So legen Sie eine Aktion für entdeckte bösartige Objekte fest

- In der Dropdown-Liste **Infiziert** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn eine mit bekanntem Virus infizierte Datei gefunden wurde.
- In der Dropdown-Liste **Verdächtig** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn eine möglicherweise infizierte Datei gefunden wurde. Im Normalfall werden solche Dateien durch Heuristik und Verhaltensanalyse erkannt.

Wenn das Installationsverzeichnis des Betriebssystems gescannt werden soll, sollten Sie für verdächtige Dateien die Aktion **Benachrichtigen** festlegen.

- In der Dropdown-Liste **Nicht desinfizierbar** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn eine mit bekanntem nicht desinfizierbarem Virus infizierte Datei gefunden wurde oder wenn die betroffene Datei nicht desinfiziert werden konnte.
- In der Dropdown-Liste **Infizierte Container** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn ein mit bekanntem Virus infizierter Dateicontainer gefunden wurde.
- In der Dropdown-Liste **Infizierte Archive** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn im Archiv eine infizierte oder verdächtige Datei gefunden wurde.
- In der Dropdown-Liste **Infizierte E-Mail-Dateien** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn eine infizierte oder verdächtige E-Mail-Datei gefunden wurde.

Wenn ein Virus bzw. ein verdächtiger Code in zusammengesetzten Objekten (Archiven, E-Mail-Dateien bzw. Container-Dateien) gefunden wird, wird die entsprechende Aktion für das ganze Objekt durchgeführt und nicht nur für den infizierten Teil des Objekts. Standardmäßig werden beim Fund solcher Objekte Benachrichtigen gesendet.

- In der Dropdown-Liste **Infizierte Bootsektoren** können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn ein Virus oder verdächtiger Code in Bootsektoren gefunden wurde.
- In den folgenden Dropdown-Listen können Sie die Aktion festlegen, die der **Scanner** ausführen soll, wenn eines der folgenden unerwünschten Programme gefunden wurde.
  - **Adware**
  - **Dialer**
  - **Scherzprogramme**
  - **Riskware**
  - **Hacktools**

Wenn Sie als Aktion **Ignorieren** festgelegt haben, erfolgen keine Aktionen: In diesem Fall wird bei einem Virenfund keine Benachrichtigung an das **Verwaltungscenter** gesendet, wie es bei der aktivierten Option **Benachrichtigen** der Fall ist.

Aktivieren Sie das Kontrollkästchen **Computer automatisch neu starten**[!], damit der Rechner des Benutzers nach dem Suchlauf automatisch neu gestartet werden kann, wenn die Desinfizierung der eventuell gefundenen schädlichen Objekte einen Neustart erfordert. Bei der deaktivierten Option wird der Rechner des Benutzers nicht neu gestartet. In der an das **Verwaltungscenter** gesendeten Statistik wird angegeben, dass der betroffene Rechner zur Desinfizierung neu gestartet werden muss. Dieser Hinweis wird in der Tabelle Status angezeigt. Alternativ kann der Administrator die betroffene Workstation über das **Verwaltungscenter** neu starten (mehr dazu finden Sie unter Antivirus-Netzwerk).

Aktivieren Sie das Kontrollkästchen **Scanfortschritt**, um den Fortschrittsbalken und Status der auf der Workstation laufenden Virensuche im **Verwaltungscenter** anzeigen zu lassen.

6.5.4.3. Einschränkungen

Die Einstellungen, die beim Scannen der Workstations unter UNIX- und Mac OS X-basierten Betriebssystemen nicht unterstützt werden, sind mit dem Zeichen [!] gekennzeichnet.

Im Bereich **Einschränkungen** sind die folgenden Scan-Einstellungen verfügbar:

- **Maximale Prüfungszeit einer Datei (ms)**. Diese Option gibt den maximalen Zeitraum in Millisekunden an, in dem ein Objekt gescannt werden kann. Nach dem Ablauf dieses Zeitraums wird der Scan des Objekts abgebrochen.
- **Maximale Rekursionstiefe**. Diese Option gibt die maximale Rekursionstiefe bei mehrfach gepackten Archiven an. Wenn die Rekursionstiefe eines zu scannenden Archivs den angegebenen Wert überschreitet, wird das Archiv nur bis zur angegebenen Rekursionsebene gescannt.
- **Maximale Archivgröße (KB)**[!]. Mit dieser Option beschränken Sie die maximale Größe (in Kilobytes) der zu scannenden Archivdateien. Wenn die Größe einer archivierten Datei den angegebenen Wert überschreitet, wird die Datei weder entpackt noch gescannt.
- **Maximale Komprimierungsrate**. Diese Option gibt die maximale Kompressionsrate archivierter Dateien an. Wenn der **Scanner** feststellt, dass der Komprimierungsfaktor einer archivierten Datei den angegebenen Wert überschreitet, wird die Datei weder entpackt noch gescannt.
- **Maximalgröße eines extrahierten Objektes (KB)**[!]. Diese Option gibt die maximale Größe einer entpackten Datei an. Wenn der **Scanner** feststellt, dass die Größe einer archivierten Datei nach dem Entpacken den angegebenen Wert überschreitet, wird die Datei weder entpackt noch gescannt.
- **Schwelle der Kompressionsprüfung (KB)**[!] . Diese Option gibt die minimale Größe (in Kilobytes) einer Datei im Archiv an, ab der der Komprimierungsfaktor geprüft werden soll.

6.5.4.4. Ausnahmen

Im Bereich **Ausnahmen** können Sie festlegen, welche Verzeichnisse und Dateien vom Scan ausgeschlossen werden sollen.

So bearbeiten Sie die Listen der vom Scan auszuschließenden Pfade und Dateien

1. Geben Sie in der Zeile **Ausgenommene Pfade und Dateien** den Pfad zur gewünschten Datei oder zum Verzeichnis an.
2. Um eine neue Zeile der Liste hinzuzufügen, klicken Sie auf und geben Sie in die geöffnete Zeile den gewünschten Pfad ein.
3. Um ein Element aus der Liste zu entfernen, klicken Sie auf neben der benötigten Zeile.

Die Liste der auszuschließenden Objekte kann die folgenden Elemente beinhalten:

1. Direkte Pfade des auszuschließenden Objektes. Beachten Sie dabei das Folgende:
   - Das Zeichen \ oder / – dieses gibt an, dass das ganze Laufwerk, auf dem sich das Installationsverzeichnis von Windows befindet, vom Scan ausgeschlossen werden soll.
   - Pfad, der mit dem Zeichen \ endet – das angegebene Verzeichnis wird vom Scan ausgeschlossen.
   - Pfad, der mit dem Zeichen \ nicht endet – ein beliebiges Unterverzeichnis, dessen Pfad mit der angegebenen Zeile beginnt, wird vom Scan ausgeschlossen.

   Beispiel: `C:\Windows` – Dateien des Verzeichnisses `C:\Windows` und seine Unterverzeichnisse vom Scan ausschließen.
2. Masken der vom Scan auszuschließenden Objekte. Bei der Festlegung von Masken können Sie die Zeichen `?` und `*` verwenden.

   Beispiel: `C:\Windows\*\*.dll` – alle Dateien, welche die Erweiterung `dll` haben und sich in allen Unterverzeichnissen des Verzeichnisses `C:\Windows` vom Scan ausschließen.
3. Reguläre Ausdrücke. Bei der Angabe der Pfade können Sie reguläre Ausdrücke verwenden. Jede Datei, deren vollständiger Name (mit der Pfadangabe) einem regulären Ausdruck entspricht, wird auch nicht gescannt.

Bevor Sie mit dem Scannen beginnen, machen Sie sich mit den Empfehlungen zum Verwenden der Antivirenprogramme auf den Rechnern unter Windows Server 2003 und Windows XP vertraut. Der entsprechende Artikel kann unter http://support.microsoft.com/kb/822158/de abgerufen werden. Dieser Artikel enthält Informationen dazu, wie Sie die Systemleistung optimieren können.

Die zur Angabe der auszuschließenden Pfade verwendeten regulären Ausdrücke haben die folgende Syntax:

```
qr{Ausdruck}Modifier
```

Am häufigsten wird der Modifier `i` verwendet. Wenn dieser Modifier gesetzt ist, wird die Groß- und Kleinschreibung ignoriert.

Unten finden Sie einige Beispiele der auszuschließenden Pfade und Dateien, die mithilfe regulärer Ausdrücke angegeben wurden:

- `qr{\\pagefile\.sys$}i` – Auslagerungsdateien von Windows NT nicht scannen.
- `qr{\\notepad\.exe$}i` – Dateien von `notepad.exe` nicht scannen.
- `qr{^C:}i` – keine Dateien und Verzeichnisse auf dem Laufwerk `C` scannen.
- `qr{^.:\\WINNT\\}i` – nichts in den auf allen Laufwerken befindlichen `WINNT`-Verzeichnissen scannen.
- `qr{(^C:)|(^.:\\WINNT\\)}i` – Vereinigung zwei oben genannter Fälle.
- `qr{^C:\\dir1\\dir2\\file\.ext$}i` – die Datei `c:\dir1\dir2\file.ext` nicht scannen.
- `qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i` – die Datei `file.ext` nicht scannen, wenn sie sich im Verzeichnis `c:\dir1\dir2` und seinen Unterverzeichnissen befindet.
- `qr{^C:\\dir1\\dir2\\}i` – das Verzeichnis `c:\dir1\dir2` und seine Unterverzeichnisse nicht scannen.
- `qr{dir\\[^\\]+}i` – das Unterverzeichnis `dir`, das sich in einem beliebigen Verzeichnis befindet, wird nicht gescannt; seine Unterverzeichnisse werden aber gescannt.
- `qr{dir\\}i` – das Unterverzeichnis `dir`, das sich in einem beliebigen Verzeichnis befindet, und seine Unterverzeichnisse nicht scannen.

Die verwendeten regulären Ausdrücke werden kurz im Dokument **Anhänge** im Anhang J. Reguläre Ausdrücke und ihre Anwendung in Dr.Web Enterprise Security Suite beschrieben.

Im Unterbereich **Inhalt folgender Dateien überprüfen** können Sie festlegen, dass zusammengesetzte Objekte nicht gescannt werden sollen. Deaktivieren Sie dafür die folgenden Optionen:

- Die Option **Archive** gibt an, dass der **Scanner** archivierte Dateien nach Viren durchsuchen soll.
- Die Option **E-Mail-Dateien** gibt an, dass E-Mail-Postfächer gescannt werden sollen.
- Die Option**Installationspakete** gibt an, dass Installationspakete durch den **Scanner** gescannt werden sollen.

6.6. Statistik zu einer Workstation anzeigen

Über das Verwaltungsmenü im Bereich **Antivirus-Netzwerk** können Sie die folgenden Informationen anzeigen lassen:

- Statistik. Wechseln Sie dazu, um Statistiken zu Aktivitäten der Antivirenkomponenten, zum Zustand der Workstations und Antivirenkomponenten anzusehen und Berichte, die alle zusammengefassten statistischen Daten oder ausgewählte Statistiktabellen enthalten, anzusehen bzw. zu speichern.
- Charts. Hier werden Diagramme mit den Informationen zu Infektionen und Bedrohungen, die auf Workstations erkannt wurden. dargestellt.
- Quarantäne. Diese Option bietet Ihnen die Möglichkeit, auf die **Quarantäne** einer Workstation remote zuzugreifen.

6.6.1. Statistik

So lassen Sie Tabellen anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
2. Wählen Sie im Verwaltungsmenü unter dem Unterbereich **Statistik** den gewünschten Punkt aus.

Der Bereich **Statistik** beinhaltet die folgenden Punkte:

- **Gesamtstatistik**. Hier finden Sie die sitzungsunabhängige Gesamtstatistik.
- Gesamtdaten. Dieser Punkt dient zur Anzeige und zum Speichern von Berichten, die alle zusammengefassten statistischen Daten bzw. Informationen aus der ausgewählten Statistiktabellen enthalten. Dieser Punkt wird nicht im Menü angezeigt, wenn alle anderen Menüpunkte im Bereich **Statistik** ausgeblendet sind.
- **Bedrohungen**. In diesem Bereich können Sie Informationen über Virenfunde (darunter Liste der infizierten Objekte, Information zu erkannten Viren und zu jeweils vom Antivirusprogramm ausgeführten Aktionen usw.) finden.
- **Fehler**. In diesem Bereich werden alle Scanfehler aufgelistet, die innerhalb des angegebenen Zeitraums auf der ausgewählten Workstation auftraten.
- Scan-Statistik. Hier finden Sie Statistiken zu den Antivirenkomponenten der ausgewählten Workstation.
- **Start/Herunterfahren**. Dieser Punkt dient zur Anzeige der Liste der Komponenten, die auf der jeweiligen Workstation früher gestartet wurden.
- **Statistiken zu Bedrohungen**. In diesem Bereich werden alle auf der gewünschten Workstation erkannten Bedrohungen nach Virentyp sortiert angezeigt.
- Status. Hier werden alle ungewöhnlichen Zustände der Workstations registriert, auf die Sie achten sollten.
- **Aufgaben**. In diesem Bereich werden Aufgaben aufgelistet, die innerhalb des angegebenen Zeitraums auf der ausgewählten Workstation ausgeführt werden sollen.

- **Produkte**. Nutzen Sie diesen Bereich, um eine Übersicht über die auf den ausgewählten Workstations installierten Produkte zu bekommen. Gemeint sind in diesem Fall Produkte vom Repository des **Servers**.
- **Virendatenbanken**. Dieser Bereich enthält Informationen zu den installierten Virendatenbanken, darunter Namen der Virendatenbank-Datei, Version der Virendatenbank; Anzahl der Virensignaturen sowie Erstellungsdatum der Virendatenbank. Dieser Punkt ist nur für Workstations verfügbar.
- **Module**. In diesem Bereich finden Sie detaillierte Informationen zu allen Modulen von **Dr.Web**, darunter ihre Beschreibung und Namen, ausführbare Datei und Vollversion eines bestimmten Moduls, u. ä. Dieser Punkt ist nur für Workstations verfügbar.
- **Alle Netzwerkinstallationen**. Hier wird die Liste mit der Installationen des **Agents** auf Workstations oder Gruppen von Workstations angezeigt.
- **Alle Deinstallationen**. Hier werden alle Workstations aufgelistet, auf denen die Antivirensoftware von **Dr.Web** deinstalliert wurde.

Um ausgeblendete Punkte des Bereichs **Statistik** anzeigen zu lassen, wählen Sie im Hauptmenü den Punkt **Administrierung** und dann im Verwaltungsmenü den Punkt **Dr.Web Server-Konfiguration**. Aktivieren Sie auf der Registerkarte **Statistik** die jeweiligen Kontrollkästchen (s. unten), klicken Sie anschließend auf **Speichern** und starten Sie den **Server** neu.

Tabelle 6-9: Übereinstimmung zwischen den Punkten des Statistik-Bereichs und Kontrollkästchen im Bereich statistischer Daten

Punkte des Statistik-Bereiches	Kontrollkästchen im Bereich statistischer Daten
Gesamtstatistik	Scan-Statistik
Bedrohungen	Erkannte Sicherheitsbedrohungen
Fehler	Scan-Fehler
Scan-Statistik	Scan-Statistik
Start/Herunterfahren	Start/Beenden der Komponenten
Statistiken zu Bedrohungen	Erkannte Sicherheitsbedrohungen
Status	Status der Workstations
Aufgaben	Verlauf der Aufgabenausführung
Virendatenbanken	Status der Workstations Status der Virendatenbanken Verlauf der Aufgabenausführung
Module	Liste der Module der Workstations
Alle Netzwerkinstallationen	Installationen des Agents

Alle Fenster, in denen Sie Aktivitäten der Antivirenkomponenten und Gesamtstatistik zur Workstation ansehen können, haben die gleiche Oberfläche und lassen sich ebenfalls identisch bedienen.

In den nächsten Abschnitten finden Sie einige Beispiele dafür, wie Sie die Gesamtstatistik über das **Verwaltungscenter** ansehen können.

6.6.1.1. Gesamtdaten

So lassen Sie zusammengefasste Informationen anzeigen

1. Wählen Sie in der hierarchischen Liste die gewünschte Workstation oder Gruppe.
2. Wählen Sie im Verwaltungsmenü im Bereich **Statistik** den Punkt **Gesamtdaten**.
3. Das Fenster mit statistischen Tabellendaten wird angezeigt. Um bestimmte statistische Daten in den Bericht aufzunehmen, klicken Sie auf der Symbolleiste auf **Gesamtdaten** und wählen Sie in der Dropdown-Liste die gewünschten Typen aus: **Scan-Statistik**, **Infektionen**, **Aufgaben**, **Start/ Herunterfahren**, **Fehler**. Statistische Daten, die in diese Bereiche des Berichts eingefügt werden, stimmen mit den Statistiken in den jeweiligen Punkten des Bereichs **Tabellen** überein. Um den Bericht mit den ausgewählten Tabellen anzuzeigen, klicken Sie auf **Aktualisieren**.
4. Um Daten für einen bestimmten Zeitraum anzeigen zu lassen, wählen Sie in der Dropdown-Liste den anzuzeigenden Zeitraum relativ zum jeweils aktuellen Tag an, oder geben Sie auf der Symbolleiste einen beliebigen Zeitraum an. Im letzten Fall müssen Sie die gewünschten Datumsangaben manuell eingeben oder auf das Kalendersymbol neben den Datumsfeldern klicken. Klicken Sie zur Anzeige der Daten auf **Aktualisieren**.
5. Um den Bericht auszudrucken oder später zu bearbeiten, klicken Sie eine der folgenden Schaltflächen an:

   Daten in der CSV-Datei speichern.

   Daten in der HTML-Datei speichern.

   Daten in der XML-Datei speichern.

   Daten in der PDF-Datei speichern.

6.6.1.2. Scan-Statistik

So lassen Sie Statistiken zu Antivirenkomponenten einer Workstation anzeigen

1. Wählen Sie in der hierarchischen Liste die gewünschte Workstation oder Gruppe.

   Wenn Sie statistischen Informationen zu mehreren Workstations oder Gruppen ansehen wollen, klicken Sie auf diese, indem Sie die STRG- oder UMSCHALTTASTE gedrückt halten.

2. Wählen Sie im Verwaltungsmenü im Bereich **Statistik** den Punkt **Scan-Statistik**.
3. Das Fenster mit den statistischen Daten wird geöffnet. Standardmäßig wird die Statistik für die letzten 24 Stunden angezeigt.
4. Um Daten für einen bestimmten Zeitraum anzeigen zu lassen, wählen Sie in der Dropdown-Liste den anzuzeigenden Zeitraum relativ zum jeweils aktuellen Tag an, oder geben Sie auf der Symbolleiste einen beliebigen Zeitraum an. Im letzten Fall müssen Sie die gewünschten Datumsangaben manuell eingeben oder auf das Kalendersymbol neben den Datumsfeldern klicken. Um Daten zu laden, klicken Sie auf **Aktualisieren** Die statistischen Daten werden im Fenster angezeigt.
5. Im Bereich **Gesamtstatistik** finden Sie die folgenden zusammengefassten Informationen:
   - Bei der Auswahl von Workstations werden Informationen zu diesen Workstations angezeigt.
   - Bei der Auswahl von Gruppen werden Informationen nach Gruppen sortiert angezeigt. Wenn mehrere Gruppen ausgewählt sind, werden nur Gruppen mit Workstations angezeigt.
   - Bei der Auswahl von Workstations und Gruppen werden Informationen für jede Workstation angezeigt, darunter auch Workstations, die zu den ausgewählten nicht leeren Gruppen gehören.

6. Um ausführliche statistische Informationen zu einer Antivirenkomponente anzuzeigen, klicken Sie in der Tabelle auf den Namen der gewünschten Workstation. Wenn Gruppen ausgewählt wurden, klicken Sie in der Tabelle mit der Gesamtstatistik auf den Namen der Gruppe und dann auf den Namen der Workstation. Das Fenster (oder ein Bereich des geöffneten Fensters) mit detaillierten statistischen Informationen wird angezeigt.
7. Über die Tabelle mit der Statistik zu den Antivirenkomponenten der Workstation oder Gruppe können Sie das Einstellungsfenster einer bestimmten Antivirenkomponente öffnen. Klicken Sie dafür in der Tabelle auf den Namen der gewünschten Komponente.
8. Um Daten in einer Spalte der Tabelle zu sortieren, klicken Sie auf den Pfeil (absteigend oder ansteigend) in der Überschrift der Spalte.
9. Um die Tabelle auszudrucken oder später zu bearbeiten, klicken Sie eine der folgenden Schaltflächen an:

   Daten in der CSV-Datei speichern.

   Daten in der HTML-Datei speichern.

   Daten in der XML-Datei speichern.

   Daten in der PDF-Datei speichern.
10. Um die sitzungsunabhängige zusammengefasste Statistik zu erhalten, klicken Sie im Verwaltungsmenü auf den Punkt **Gesamtstatistik**. Das Fenster mit der Gesamtstatistik wird angezeigt.
11. Um die Statistik zu erkannten Bedrohungen in Form von Diagrammen darstellen zu lassen, wählen Sie im Verwaltungsmenü den Punkt **Charts**. Das Fenster mit den Diagrammen wird angezeigt (mehr dazu finden Sie im nächsten Abschnitt).

6.6.1.3. Status

So lassen Sie den Zustand einer Workstation anzeigen

1. Wählen Sie in der hierarchischen Liste die gewünschte Workstation oder Gruppe.
2. Wählen Sie im Verwaltungsmenü im Bereich **Statistik** den Punkt **Status**.
3. Der Zustand von Workstations wird im Fenster automatisch entsprechend den auf der Symbolleiste festgelegten Einstellungen angezeigt.
4. Um nur Benachrichtigungen zum Zustand eines bestimmten Schweregrads anzeigen zu lassen, wählen Sie auf der Symbolleiste in der Dropdown-Liste **Schweregrad** den gewünschten Schweregrad aus. Der Vorgabewert ist **Minimal**: Die Liste wird komplett angezeigt.
5. In die Liste werden auch Workstations aufgenommen, die keine Verbindung mit dem **Server** innerhalb eines bestimmten Zeitraums herstellten. Geben Sie im Feld links von der Liste **Schweregrad** die Anzahl von Tagen an. Wenn dieser Wert überschrittet ist, wird dieses Ereignis als kritisch eingestuft, und die entsprechende Meldung wird im Fenster des Bereichs **Status** ausgegeben.
6. Die Anzeige dieser Tabelle lässt sich wie die Anzeige der oben beschriebenen Statistik-Tabelle anpassen.

Sie können statistische Informationen zu mehreren Workstations ansehen. Wählen Sie dafür in der hierarchischen Liste des Netzwerks die gewünschten Workstations aus.

6.6.2. Charts

Diagramme für Infektionen

So lassen Sie Diagramme mit Details zu erkannten Infektionen anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe. Wählen Sie im geöffneten Verwaltungsmenü unter **Allgemein** den Punkt **Charts**.
2. Das angezeigte Fenster enthält die folgenden Diagrammdaten:
   - **Top 10 Viren**. Hier werden zehn Viren aufgelistet, welche die höchste Anzahl von Dateien infizierten. Im Diagramm wird die Anzahl von Objekten, die durch die angegebenen Viren infiziert wurden, angezeigt.
   - **Tägliche Virenaktivität**. Der angegebene Zeitraum wird in 24 Stunden aufgeteilt. Im Diagramm wird die Gesamtzahl von Viren angezeigt, die innerhalb von 24 Stunden Tag in allen ausgewählten Netzwerkobjekten (auf Workstations und in Gruppen) erkannt wurden. Dieses Diagramm ist nur dann verfügbar, falls der angegeben Zeitraum mehr als 24 Stunden beträgt.
   - **Infektionsklassen**. Hier wird die Anzahl von Objekten angezeigt, die vom jeweiligen Infektionstyp infiziert wurden.
   - **Nach Anzahl der infizierten Stationen in der Gruppe**. Hier wird die Anzahl von infizierten Workstations für jede Gruppe angezeigt, die solche Workstations enthält.
   - **Ausgeführte Aktionen**. Hier wird die Anzahl von infizierten Objekten angezeigt, die durch die Antivirensoftware entsprechend behandelt wurden.
3. Um Diagrammdaten für einen bestimmten Zeitraum angezeigt zu bekommen, wählen Sie auf der Symbolleiste in der Dropdown-Liste einen Zeitraum: Tag oder Monat. Sie können auch einen beliebigen Zeitraum angeben. Im letzten Fall müssen Sie die gewünschten Datumsangaben manuell eingeben oder auf das Kalendersymbol neben den Datumsfeldern klicken. Klicken zur Anzeige der Daten auf **Aktualisieren**.

Diagramme für die Gesamtstatistik

Die Diagrammdaten werden im Punkt **Charts** des Bereiches **Allgemein** sowie in einigen Punkten des Bereiches **Statistik** im Verwaltungsmenü angezeigt.

Je nach dem in der hierarchischen Liste jeweils ausgewählten Objekt (Workstation oder Gruppe) werden unterschiedliche Diagrammen angezeigt. In der Tabelle unten werden alle möglichen Diagramme und die Bereiche des Verwaltungsmenüs, in denen diese Diagramme angezeigt werden, je nach dem ausgewählten Objekt angezeigt.

Tabelle 6-10: Übereinstimmung zwischen den Diagrammen und ausgewählten Punkten in der hierarchischen Liste sowie Bereichen des Verwaltungsmenüs

Diagramme	Für Gruppen	Für Workstations	Bereiche
Top 10 Viren	+	+	Infektionen Viren Charts
Top 10 infizierter PCs	+		Infektionen
Infektionsarten	+	+	Viren
Installationsergebnisse			Alle Netzwerkinstallationen
Durchschnittliche Infektionsaktivität	+		Scan-Statistik
Nach der Fehleranzahl	+	+	Fehler

Diagramme	Für Gruppen	Für Workstations	Bereiche
Fehler nach Komponenten	+	+	Fehler
Ergebnisse der Aufgabenausführung	+	+	Aufgaben
Infektionsklassen	+	+	Charts
Ausgeführte Aktionen	+	+	Charts
Tägliche Virenaktivität	+	+	Charts
Nach Anzahl der infizierten Stationen in der Gruppe	+		Charts

- **Top 10 infizierter PCs**. Hier werden zehn am meisten infizierten Workstations aufgeführt. Im Diagramm wird die Anzahl von schädlichen Objekten, die auf den angegebenen Workstations gefunden wurden, angezeigt.
- **Infektionsarten**. Im Kreisdiagramm wird die Anzahl von erkannten schädlichen Objekten nach Objekttyp sortiert angezeigt
- **Installationsergebnisse**. Im Kreisdiagramm wird die Anzahl aller Installationen, die von diesem **Server** her gestartet wurden, nach Installationsergebnissen sortiert angezeigt. Bei fehlgeschlagenen Installationen werden auch Fehlerursachen angezeigt. Das Diagramm wird für alle Installationen, die von diesem **Server** initiiert wurden, unabhängig von dem in der Liste ausgewählten Objekt angezeigt.
- **Durchschnittliche Infektionsaktivität**. Hier wird die durchschnittliche Infizierungsrate auf den Workstations der ausgewählten Gruppe angezeigt. Dieser Wert wird berechnet aus der Summe aller gefundenen bösartigen Objekte, dividiert durch die Anzahl der auf jeder Workstation gescannten Objekte.
- **Nach der Fehleranzahl**. Hier werden Workstations aufgelistet, auf denen die installierten Antivirenkomponenten ihre Aufgaben nicht funktionsgerecht bewältigen. Das Diagramm zeigt die Anzahl von Fehlern nach Workstations sortiert an.
- **Fehler nach Komponenten**. Hier werden die auf den Workstations installierten Antivirenkomponenten aufgelistet, bei denen Probleme auftreten. Im Kreisdiagramm wird die Gesamtzahl der Fehler je nach Komponente angezeigt.
- **Ergebnisse der Aufgabenausführung**. Hier werden Aufgaben aufgelistet, die für die ausgewählten Objekte ausgeführt wurden. Im Diagramm wird angezeigt, wie oft jede der Aufgaben gestartet wurde. In der Tabelle unter dem Diagramm werden auch die entsprechenden Ergebnisse angezeigt.

6.6.3. Quarantäne

Inhalt der Quarantäne

Sie können Dateien in die **Quarantäne** wie folgt verschieben:

- Durch eine der Antivirenkomponenten, beispielsweise durch den **Scanner**.
- Manuell durch Benutzer über den **Quarantäne**-Manager.

Die in **Quarantäne** verschobenen Dateien werden automatisch erneut gescannt. Dabei achten Sie auf das Folgende:

- Es wird genau festgestellt, ob das Objekt wirklich infiziert wurde. Eventuell wird auch der Typ der Bedrohung erkannt (da die Information zum Infizierungsstatus einer Datei beim manuellen Verschieben in die **Quarantäne** nicht verfügbar ist).
- Namen von Infektionen sowie deren Type werden in eine einheitliche Form gebracht.

Benutzer können die Dateien in der **Quarantäne** über das **Verwaltungscenter** bzw. über den **Quarantäne**–Manager erneut scannen lassen.

So bearbeiten Sie den Inhalt der Quarantäne über das Verwaltungscenter

1. Wählen Sie im Hauptmenü des **Verwaltungscenters den Punkt** **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe. Wählen Sie im Verwaltungsmenü unter **Allgemein** den Punkt **Quarantäne**.
2. Das Fenster mit den Tabellendaten über den aktuellen Status der **Quarantäne** wird geöffnet.

   Wenn nur eine Workstation ausgewählt wurde, wird eine Tabelle mit den Objekten, die sich auf dieser Workstation in der **Quarantäne** befinden, angezeigt.

   Wenn mehrere Workstations, eine Gruppe bzw. mehrere Gruppen ausgewählt wurden, werden mehrere Tabellen, die Informationen zu den Objekten in der Quarantäne auf jeder der Workstations enthalten, angezeigt.
3. Um Dateien, die innerhalb eines bestimmten Zeitraums in die **Quarantäne** verschoben wurden, angezeigt zu bekommen, geben Sie auf der Symbolleiste den gewünschten Zeitraum an und klicken Sie auf **Aktualisieren**.
4. Um Dateien, die sich in der **Quarantäne** befinden, zu verwalten, aktivieren Sie das Kontrollkästchen neben der entsprechenden Datei, Gruppe von Dateien bzw. neben allen Dateien in der **Quarantäne** (im Tabellentitel). Wählen Sie auf der Symbolleiste eine der folgenden Aktionen aus:

   - **Dateien wiederherstellen** – Dateien aus der **Quarantäne** wiederherstellen.

   Verwenden Sie diese Funktion nur dann, wenn Sie sicher sind, dass das Objekt nicht infiziert ist.

   Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus:

   a) **Dateien wiederherstellen** – Dateien am ursprünglichen Speicherort wiederherstellen. Die jeweilige Datei wird in dem Verzeichnis, in dem sie sich vor der Verschiebung in die **Quarantäne** befand, wiederhergestellt.

   b) **Dateien mit dem angegebenen Pfad wiederherstellen** – Datei in das vom Administrator angegebenen Verzeichnis verschieben.

   - **Dateien löschen** – ausgewählte Dateien aus der **Quarantäne** und vom System löschen.
   - **Dateien prüfen** – ausgewählte Dateien in der **Quarantäne** erneut scannen.
   - **Export** – in der **Quarantäne** ausgewählte Dateien kopieren und speichern.

   Nachdem verdächtige Dateien in die lokale **Quarantäne** auf der Rechner verschoben sind, können Sie diese Dateien über das **Verwaltungscenter** kopieren und mithilfe eines Webbrowsers speichern, um diese später an das Virenlabor von **Dr.Web** zur Analyse zu versenden. Um Dateien zu speichern, aktivieren Sie die Kontrollkästchen neben den gewünschten Dateien und klicken Sie auf **Export**.

   - Exportieren Sie Informationen zum Zustand der **Quarantäne** in eine Datei. Für den Export stehen die folgenden Formate zur Verfügung:

   Daten in der CSV-Datei speichern.

   Daten in der HTML-Datei speichern.

   Daten in der XML-Datei speichern.

   Daten in der PDF-Datei speichern.

6.7. Installationsdateien versenden

Beim Einrichten eines neuen Workstation-Kontos wird im **Verwaltungscenter** ein Installationspaket des **Dr.Web Agents** generiert. Das Installationspaket besteht aus dem **Dr.Web Agent** und einem Parametersatz, der die Einstellungen für die Verbindung mit dem **Dr.Web Server** und für die Autorisierung am **Dr.Web Server** beinhaltet. Eine detaillierte Beschreibung des Installationspakets und der Installation des **Agents** finden Sie in der **Installationsanleitung** im Abschnitt Dr.Web Agent lokal installieren.

Sie können generierte Installationspakete an Benutzer per E-Mail problemlos versenden.

Der Inhalt einer E-Mail beim Versand von Installationspaketen wird folgendermaßen generiert:

1. Betriebssystem der Workstation ist bekannt:
   a) Windows: Der E-Mail wird ein Installationspaket des **Dr.Web Agents für Windows** beigefügt.
   b) Linux, Mac OS X, Android: Der E-Mail wird eine Installationsdatei des **Dr.Web Agents** für das jeweilige Betriebssystem und eine Konfigurationsdatei mit den Einstellungen für die Verbindung mit dem **Dr.Web Server** beigefügt.
2. Das Betriebssystem der Workstation ist nicht bekannt (es handelt sich um ein neues Workstation-Konto, der **Agent** ist noch nicht installiert):
   a) Wenn der **Server** keine Installationspakete für Workstations unter Linux, OS Mac X, Android besitzt (insbesondere wenn der **Server** keine installierte zusätzliche Distribution (extra) hat): Der E-Mail werden ein Installationspaket des **Dr.Web Agents für Windows** und eine Konfigurationsdatei mit den Einstellungen für die Verbindung mit dem **Dr.Web Server** für Workstations unter Linux, OS Mac X, Android beigefügt.
   b) Wenn der **Server** mindestens ein Nicht-Windows-Installationspaket besitzt: Der E-Mail werden ein Installationspaket des **Dr.Web Agents für Windows**, eine Konfigurationsdatei mit den Einstellungen für die Verbindung mit dem **Dr.Web Server** für Workstations unter Linux, OS Mac X, Android sowie der Link zum Herunterladen von Installationsdateien für Workstations unter Linux, OS Mac X, Android beigefügt.

So versenden Sie Installationspakete per E-Mail

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Bereich **Antivirus-Netzwerk**. Wählen Sie in der hierarchischen Liste des geöffneten Fensters die folgenden Objekte aus:
   - Wählen Sie eine Workstation aus, um ein für die Workstation generiertes Installationspaket per E-Mail zu versenden.
   - Wählen Sie eine Gruppe von Workstations aus, um alle für die Workstations dieser Gruppe generierten Installationspaket per E-Mail zu versenden.

   Zur Mehrfachauswahl verwenden Sie die STRG- oder UMSCHALTTASTE.
2. Klicken Sie in der Symbolleiste auf **Allgemein** → **Installationsdateien versenden**.
3. Legen Sie im geöffneten Bereich **Versenden von Installationsdateien** die folgenden Einstellungen fest:
   - Geben Sie im Bereich **E-Mail-Adressen der Empfänger** E-Mail-Adressen an, an die das Installationspaket versendet werden soll. Wenn Sie mehrere Workstations oder Gruppen ausgewählt haben, geben Sie neben dem Namen jeder gewünschten Workstation die E-Mail-Adresse zum Versand von Installationspaketen an.
   - Aktivieren Sie im Bereich **Erweitert** das Kontrollkästchen **In ein ZIP-Archiv packen**, um Dateien der Installationspaketen in ein ZIP-Archiv zu verpacken. Das Verpacken macht dann Sinn, wenn der E-Mail-Client des Benutzers mit Filtern ausgestattet ist, welche die Übertragung von ausführbaren Dateien in E-Mail-Anhängen eventuell nicht zulassen.
   - Geben Sie im Bereich **Absender** die E-Mail-Adresse an, die als Absender für E-Mails mit Installationsdateien verwendet werden soll.

- Geben Sie im Bereich **Einstellungen des SMTP-Servers** die Einstellungen des SMTP-Servers an, der zum Versand von E-Mails verwendet werden soll. Wenn diese Einstellungen bereits bekannt sind bzw. früher festgelegt wurden, wird dieser Bereich reduziert. Sie können bei Bedarf ihn wieder erweitern und entsprechend konfigurieren. Beim ersten Versand von Installationspaketen müssen Sie die folgenden Einstellungen konfigurieren:
  - **Adresse**. Geben Sie hier die Adresse des SMTP-Servers an, der zum Versand von E-Mails verwendet werden soll.
  - **Port**. Geben Sie hier den Port des SMTP-Servers an, der zum Versand von E-Mails verwendet werden soll.
  - **Benutzer**, **Passwort**. Geben Sie hier den Namen und das Passwort vom Benutzer des SMTP-Servers an, wenn eine Autorisierung auf dem SMTP-Server erforderlich ist.
  - Aktivieren Sie das Kontrollkästchen **STARTTLS-Verschlüsselung**, um die *STARTTLS*-Verschlüsselung des Datenverkehrs beim Versand von E-Mails zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **SSL-Verschlüsselung**, um die *SSL*-Verschlüsselung des Datenverkehrs beim Versand von E-Mails zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **CRAM-MD5-Authentifizierung verwenden**, um die *CRAM-MD5*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **DIGEST-MD5-Authentifizierung verwenden**, um die *DIGEST-MD5*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **Übliche Authentifizierung verwenden**, um die *Plaintext*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **LOGIN-Authentifizierung verwenden**, um die *LOGIN*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **Richtigkeit des SSL-Zertifikats des Servers überprüfen**, um das SSL-Zertifikat des Servers auf Richtigkeit zu überprüfen.
  - Aktivieren Sie das Kontrollkästchen **Testbetrieb**, um SMTP-Sitzungen zu protokollieren.Klicken Sie auf **Senden**.

6.8. Nachrichten an Workstations unter Windows® versenden

Der Systemadministrator kann an Benutzer Nachrichten mit beliebigem Inhalt versenden. Diese Nachrichten enthalten die folgenden Elemente:

- Text der Nachricht;
- Hyperlinks auf Web-Ressourcen;
- Firmenlogo (oder andere Grafik);
- Im oberen Teil der Nachricht wird auch das Datum angezeigt, an dem die Nachricht angekommen ist.

Diese Nachrichten werden auf Workstations als Popup-Fenster angezeigt (s. die Abb. 6-1).

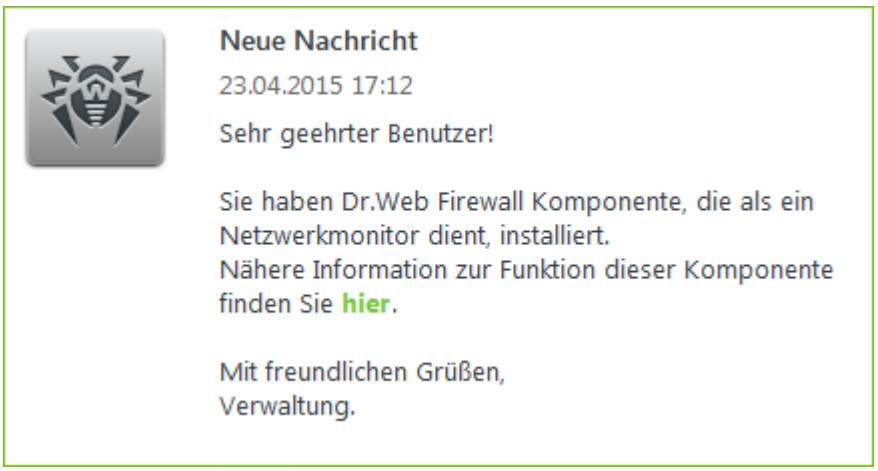

Neue Nachricht
23.04.2015 17:12
Sehr geehrter Benutzer!
Sie haben Dr.Web Firewall Komponente, die als ein Netzwerkmonitor dient, installiert.
Nähere Information zur Funktion dieser Komponente finden Sie hier.
Mit freundlichen Grüßen,
Verwaltung.

Abbildung 6-1. Nachrichtenfenster auf Workstations

So versenden Sie Nachrichten an Benutzer

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie in der hierarchischen Liste des angezeigten Fensters eine Workstation oder Gruppe von Workstations und klicken Sie auf der Symbolleiste auf **Allgemein** → **Nachrichten an Stationen senden**.
3. Füllen Sie im nächsten Fenster die folgenden Felder aus:
   - **Nachrichtentext**. Das ist ein Pflichtfeld. Hier wird der Text der Nachricht eingegeben.
   - Aktivieren Sie das Kontrollkästchen **Logo in der Nachricht anzeigen**, damit eine Grafik im oberen Teil des Nachrichtenfensters angezeigt wird. Legen Sie für das Logo die folgenden Einstellungen fest:
     - Aktivieren Sie das Kontrollkästchen **Transparenz verwenden**, um das Firmenlogo mit Transparenz durchsichtig wirken zu lassen (s. dazu Format der Logodatei, den Punkt 4).
     - Sie können im Feld **URL** einen Link auf die Webseite, die beim Anklicken des Logos geöffnet wird, angeben.
     - Sie können bei Bedarf im Feld **Nachrichtentitel** einen Titel für die Nachricht, z. B. Firmennamen, angeben. Dieser Text wird im oberen Teil des Nachrichtenfensters rechts vom Logo angezeigt. Wenn Sie dieses Feld leer lassen, werden an dieser Stelle des Nachrichtenfensters Informationen zur Nachricht angezeigt.
     - Klicken Sie rechts vom Feld **Logo-Datei** die Schaltfläche an, um eine Logodatei von der lokalen Ressource zu laden, oder wählen Sie im erscheinenden Fenster vom Explorer das gewünschte Objekt (s. dazu Format der Logodatei).

   Wenn Sie kein Logo gewählt haben, bzw. die Größe des Logos den maximal zulässigen Wert überschreitet (s. Format der Logodatei, den Punkt 3), wird an seiner Stelle im Nachrichtenfenster das Symbol des **Dr.Web Agents** angezeigt.
   - Aktivieren Sie das Kontrollkästchen **Link in der Nachricht anzeigen**, um zur Nachricht einen Link auf eine Webseite hinzuzufügen.

   So fügen Sie einen Link hinzu

   1. Geben Sie im Feld **URL** den Link auf die gewünschte Webseite an.
   2. Geben Sie im Feld **Text** den Text an, der mit dem Link verknüpft wird.
   3. Fügen Sie im Feld **Nachrichtentext** das Tag `{link}` an allen Stellen ein, wo Sie einen Link hinzufügen wollen. Im Schlusstext der Nachricht erscheinen an diesen Stellen die entsprechenden Links. Die Anzahl der Tags `{link}` in einem Text ist begrenzt. All diese Tags werden die gleichen Werte aus den Feldern **URL** und **Text** enthalten.

- Aktivieren Sie das Kontrollkästchen **Nur an Online-Stationen senden**, um Nachrichten nur an aktive Workstations (online) zu versenden. Bei der aktivierten Option werden keine Nachrichten an nicht aktive Workstations versendet. Bei der deaktivierten Option werden Nachrichten an nicht aktive Workstations erst dann versendet, sobald sie wieder in Netzwerk verfügbar sind.
- Aktivieren Sie das Kontrollkästchen **Versandstatus anzeigen**, um Benachrichtigungen über den Status der versendeten Nachrichten anzuzeigen.

4. Klicken Sie auf **Senden**.

Format der Logodatei

Eine Bilddatei, die als Logo in der Nachricht verwendet wird, muss die folgenden Anforderungen erfüllen:

1. Mögliche Grafikformate: BMP, JPG, PNG, GIF, SVG.
2. Die Größe der Logodatei darf 512 KB nicht überschreiten.
3. Die Bildgröße ist 72x72 Pixel. Bilder anderer Auflösungen werden auf die Standardauflösung skaliert.
4. Bittiefe (bit depth) von 8 bis 24 Bit.

Wenn Sie einen transparenten Hintergrund auf Ihrem Logo haben wollen, verwenden Sie dafür PNG- oder GIF-Dateien.

Bevor Sie Nachrichten massenhaft versenden, ist es empfehlenswert, eine erstellte Nachricht zuerst an einen Rechner mit dem installierten **Agent** zu versenden. So stellen Sie sicher, dass alles richtig konfiguriert wurde.

Beispiel einer Nachricht

Um die in der Abbildung 6-0 dargestellte Nachricht zu senden, wurden folgende Parameter festgelegt:

Nachrichtentext:

```
Sehr geehrter Benutzer!


Sie haben Dr.Web Firewall Komponente, die als ein Netzwerkmonitor dient,
installiert.
Nähere Informationen zur Funktionen dieser Komponente finden Sie {link}.


Mit freundlichen Grüßen,
Verwaltung.
```

URL: `http://drweb.com/`

Text: `hier`

Kapitel 7: Dr.Web Server konfigurieren

In diesem Kapitel finden Sie detaillierte Anweisungen für die Verwaltung des Antivirus-Netzwerks und des **Dr.Web Servers**. Dieses Kapitel ist in die folgenden Abschnitte unterteilt:

- Protokollierung. In diesem Abschnitt lernen Sie, wie Sie Protokolle des **Servers** sowie detaillierte statistische Daten zum **Server** angezeigt bekommen und sie verwalten.
- Dr.Web Server konfigurieren. In diesem Abschnitt wird die Konfiguration der Einstellungen des **Servers** beschrieben.
- Zeitplan des Dr.Web Servers konfigurieren. Lesen Sie diesen Abschnitt durch, wenn Sie Aufgaben zur Wartung des **Servers** planen wollen.
- Webserver konfigurieren. In diesem Abschnitt wird die Konfiguration der Einstellungen des **Webservers** beschrieben.
- Benutzerprozeduren. Dieser Abschnitt enthält Anweisungen für die Verwendung und Konfiguration von benutzerdefinierten Prozeduren.
- Benachrichtigungen konfigurieren. In diesem Abschnitt lernen Sie, wie Sie Benachrichtigungen über bestimmte Ereignisse im Antivirus-Netzwerk konfigurieren und zukommen lassen.
- Dr.Web Server-Repository verwalten. Lesen Sie diesen Abschnitt durch, wenn Sie das Repository für die Aktualisierung aller Komponenten des Antivirus-Netzwerks über das **GUS** und anschließende Verteilung der heruntergeladenen Updates auf Workstations einstellen wollen.
- Datenbankverwaltung. Hier erfahren Sie, wie die Datenbank des **Servers** verwaltet wird.
- Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern. In diesem Abschnitt wird ein Multiserver-Antivirus-Netzwerk und seine Konfiguration beschrieben.

7.1. Protokollierung

7.1.1. Dr.Web Server-Protokoll

Im Protokoll des **Dr.Web Servers** werden dessen Aktivitäten aufgezeichnet.

Das Protokoll des **Servers** wird zum Debuggen und zur Fehlerbehebung verwendet, falls eine oder mehrere Komponenten des Antivirus-Netzwerks nicht mehr richtig ausgeführt werden.

Der Standardname der Protokolldatei ist `drwcsd.log`. Die Datei befindet sich standardmäßig unter dem folgenden Pfad:

- Unter **UNIX**-basierten Betriebssystemen:
  - Unter Linux und Solaris: `/var/opt/drwcs/log/drwcsd.log`.
  - Unter FreeBSD: `/var/drwcs/log/drwcsd.log`.
- Unter **Windows**: im Unterverzeichnis `var` des Installationsverzeichnisses vom **Server**.

Es handelt sich dabei um eine Textdatei (s. dazu das Dokument **Anhänge**, den Anhang K. Format von Protokolldateien).

So lassen Sie das Server-Protokoll über das Verwaltungscenter anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster des Verwaltungsmenüs den Punkt **Dr.Web Server-Protokoll**.

3. Das Fenster mit der Liste der Protokolle des **Servers** wird angezeigt. Entsprechend den Einstellungen des Rotationsmodus wird das folgende Format für die Benennung der Protokolldateien des **Servers** verwendet: *<file_name>*.*<N>*.log oder *<file_name>*.*<N>*.log.gz, dabei *<N>* ist die laufende Nummer: 1, 2 usw. Z. B. beim Dateinamen drwcsd sieht die Liste der Protokolldateien wie folgt aus:
   - drwcsd.log – aktuelle Datei (Datei, in der protokolliert wird),
   - drwcsd.1.log.gz – vorherige Datei,
   - drwcsd.2.log.gz und so weiter – je größer die Zahl ist, desto älter ist die Version.
4. Um Protokolldateien zu verwalten, aktivieren Sie das Kontrollkästchen neben der gewünschten Datei. Um alle Dateien auszuwählen, aktivieren Sie das Kontrollkästchen im Tabellentitel. Auf der Symbolleiste stehen Ihnen die folgenden Schaltflächen zur Verfügung:

   Ausgewählte Logdateien exportieren. Diese Option gibt an, dass die ausgewählten Dateien lokal gespeichert werden sollen. Diese Option macht dann Sinn, wenn der Inhalt des Protokolls von einem Remote-Rechner aus angesehen wird.

   Ausgewählte Logdateien löschen. Diese Option gibt an, dass die ausgewählten Protokolldateien endgültig gelöscht werden sollen.

7.2. Dr.Web Server konfigurieren

So konfigurieren Sie den Dr.Web Server

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster den Punkt **Dr.Web Server-Konfiguration**. Das Fenster zum Einstellen des **Dr.Web Servers** wird angezeigt.

> Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

3. Auf der Symbolleiste sind die folgenden Schaltflächen verfügbar:

   Dr.Web Server neu starten. Mit dieser Option können Sie den **Server** neu starten, damit die im Bereich vorgenommenen Änderungen wirksam werden. Diese Schaltfläche ist verfügbar, sobald die Änderungen an den Einstellungen vorgenommen sind und die Schaltfläche **Speichern** angeklickt wurde.

   Konfiguration aus Backup wiederherstellen. Bei dieser Option handelt es sich um eine Dropdown-Liste, die gespeicherte Kopien der Einstellungen des Bereichs enthält. Diese Einstellungen können bei Bedarf wiederhergestellt werden. Diese Schaltfläche wird anklickbar, sobald Änderungen an den Einstellungen vorgenommen wurden und die Schaltfläche **Speichern** angeklickt wurde.

   Alle Parameter mit den ursprünglichen Werten wiederherstellen. Diese Option gibt an, dass die ursprünglichen (zuletzt gespeicherten) Werte aller Einstellungen des Bereichs wiederhergestellt werden sollen.

   Defaultparameter wiederherstellen. Diese Option gibt an, dass die Standardwerte aller Einstellungen des Bereichs wiederhergestellt werden sollen.
4. Damit die Änderungen an den Einstellungen des Bereichs wirksam werden, klicken Sie auf **Speichern** und starten Sie den **Server** neu. Klicken Sie dafür auf der Symbolleiste des Bereichs auf **Dr.Web Server neu starten**.

7.2.1. Allgemein

Auf der Registerkarte **Allgemein** können Sie die folgenden Einstellungen des **Servers** konfigurieren:

- Im Feld **Name des Dr.Web Servers** wird der Name des **Servers** angegeben. Wenn das Feld leer ist, wird der Name des Rechners, auf dem der **Dr.Web Server** installiert ist, verwendet.
- Im Feld **Anzahl paralleler Anfragen** wird die Anzahl der parallelen Anfragen angegeben, welche die **Agents** versenden. Dieser Parameter beeinflusst die Leistung des **Servers**. Ändern Sie den vorgegebenen Wert nur nach Absprache mit dem Support-Team.
- Im Feld **Anzahl von Verbindungen mit der Datenbank** wird die Anzahl von Verbindungen des **Servers** mit der Datenbank angegeben. Ändern Sie den vorgegebenen Wert nur nach Absprache mit dem Support-Team.

Ab Version **10.0** kann der Parameter **Warteschlange** nicht mehr über das **Verwaltungscenter** geändert werden.

Bei der Installation des **Servers** wird der Standardwert 50 verwendet. Wenn Sie bei einer erneuten Installation die Konfigurationsdatei der alten Version verwenden, wird der Wert der Warteschlange aus dieser Datei übernommen.

Wenn Sie aber diesen Wert ändern wollen, ändern Sie den Wert des folgenden Parameters der Konfigurationsdatei des **Servers**:

```
<!-- Maximun authorization queue length -->
<maximum-authorization-queue size='50'/>
```

- Aktivieren Sie das Kontrollkästchen **Update-Traffic einschränken**, um das Volumen des Netzwerk-Datenverkehrs bei der Übertragung von Updates zwischen dem **Server** und den **Agents** einzuschränken.

  Wenn das Kontrollkästchen aktiviert ist, legen Sie im Feld **Maximale Übertragungsgeschwindigkeit (KB/s)** die maximale Bandbreite für die Übertagung von Updates fest. Updates werden dabei innerhalb der festgelegten Bandbreite des gesamten Netzwerk-Datenverkehrs aller **Agents** übertragen.

  Wenn das Kontrollkästchen deaktiviert ist, wird die Bandbreite für die Übertragung von Updates für die **Agents** nicht eingeschränkt.

  Weitere Informationen finden Sie unter Datenverbrauch von Workstations begrenzen.

- In der Dropdown-Liste **Registrierungsmodus für Anfänger** wird eine Verbindungsrichtlinie für neue Workstations gewählt (s. dazu Verbindungsrichtlinie für Workstations).
  - In der Dropdown-Liste **Standardmäßige primäre Gruppe** wird eine primäre Gruppe ausgewählt, in die Workstations verschoben werden, falls der Zugriff auf den **Server** automatisch bestätigt wird.
- Aktivieren Sie das Kontrollkästchen **Nicht autorisierte Stationen zum Anfänger machen**, um die Einstellungen für den Zugriff auf den **Server** bei nicht autorisierten Workstations zurückzusetzen. Diese Option macht dann Sinn, wenn einige Einstellungen des **Servers** (z. B. öffentlicher Schlüssel) geändert wurden oder eine andere Datenbank gewählt wurde. Workstations können in diesen Fällen keine Verbindung herstellen und müssen deshalb für den Zugriff auf den **Server** neu eingestellt werden.
- In der Dropdown-Liste **Verschlüsselung** wird eine Richtlinie für die Verschlüsselung des Datenverkehrs ausgewählt, der über den Übertragungskanal zwischen dem **Dr.Web Server** und den damit verbundenen Clients, darunter **Agents**, benachbarte **Server**, **Netzwerk-Installer**, erfolgt.

  Diese Einstellungen werden unter Datenverkehr verschlüsseln und komprimieren detailliert beschrieben.

- In der Dropdown-Liste **Komprimierung** wird eine Richtlinie für die Komprimierung des Datenverkehrs ausgewählt, der über den Übertragungskanal zwischen dem **Dr.Web Server** und den damit verbundenen Clients, darunter **Agents**, benachbarte **Server**, **Netzwerk-Installer**, erfolgt. Weitere Informationen finden Sie unter Datenverkehr verschlüsseln und komprimieren.
  - Wenn Sie **Ja** und **Möglich** für die Komprimierung des Datenverkehrs auswählen, wird die Dropdown-Liste **Komprimierungsstufe** verfügbar. In dieser Liste können Sie eine Zahl im Bereich von 1 bis 9 auswählen, wobei die Eins die minimale und die Neun die maximale Komprimierungsstufe ist.
- Im Feld **Zulässige Differenz zwischen der Zeit des Servers und des Agenten** wird die zulässige Differenz zwischen der Systemzeit des **Dr.Web Servers** und der **Dr.Web Agents** in Minuten angegeben. Wenn die Differenz höher als angegeben ist, wird dies in dem Status der Workstation auf dem **Dr.Web Server** markiert. Der Standardwert beträgt 3 Minuten. Der Wert 0 bedeutet, dass keine Überprüfung durchgeführt wird.
- Aktivieren Sie das Kontrollkästchen **IP-Adressen ersetzen**, um in der Protokolldatei des **Dr.Web Servers** IP-Adressen durch DNS-Namen von Rechnern zu ersetzen.
- Aktivieren Sie das Kontrollkästchen **NetBIOS-Namen ersetzen**, um im Verzeichnis des Antivirus-Netzwerks im **Verwaltungscenter** nicht NetBIOS-Namen von Workstations, sondern ihre DNS-Namen anzeigen zu lassen. Wenn Domänennamen nicht festgestellt werden können, werden IP-Adressen angezeigt.

Standardmäßig sind die Kontrollkästchen **IP-Adressen ersetzen** und **NetBIOS-Namen ersetzen** deaktiviert. Wenn der DNS-Dienst falsch konfiguriert ist, kann die Aktivierung dieser Optionen die Leistung des **Servers** erheblich beeinträchtigen. Wenn Sie eine oder beide Optionen aktivieren, sollten Sie auf dem DNS-Server die Zwischenspeicherung von Namen aktivieren.

Wenn das Kontrollkästchen **NetBIOS-Namen ersetzen** aktiviert ist und ein **Proxy-Server** im Antivirus-Netzwerk verwendet wird, wird der Name des Rechners, auf dem der **Proxy-Server** installiert ist, für alle Workstations, die mit dem **Server** über den **Proxy-Server** verbunden sind, im **Verwaltungscenter** verwendet.

- Aktivieren Sie das Kontrollkästchen **Beschreibungen der Workstations synchronisieren**, um die Beschreibung des Benutzerrechners mit der Beschreibung der Workstation im **Verwaltungscenter** (im Feld **Computer description** auf der Seite **System properties**) zu synchronisieren. Wenn die Beschreibungen der Workstations im **Verwaltungscenter** fehlt, wird in dieses Feld die Beschreibung des Benutzerrechners eingetragen. Wenn die Beschreibungen nicht identisch sind, wird die Beschreibung im **Verwaltungscenter** durch die Beschreibung des Benutzerrechners ersetzt.
- Aktivieren Sie das Kontrollkästchen **Epidemien verfolgen**, damit der Administrator benachrichtigt wird, wenn die Anzahl gefundener Viren extrem hoch ist. Wenn das Kontrollkästchen deaktiviert ist, wird der Administrator im normalen Modus benachrichtigt. Bei der aktivierten Option können Sie die folgenden Einstellungen festlegen:
  - **Periode (Sek.)**. Hier wird der Zeitraum in Sekunden angegeben, innerhalb dessen eine festgelegte Anzahl von Nachrichten über die erkannten Infektionen empfangen werden muss, so dass **Dr.Web Server** an den Administrator eine einheitliche Epidemie-Benachrichtigung sendet.
  - **Nachrichtenanzahl**. Hier wird die Anzahl von Nachrichten über die erkannten Infektionen angegeben, die innerhalb eines festgelegten Zeitraums empfangen werden müssen, so dass **Dr.Web Server** an den Administrator eine einheitliche Epidemie-Benachrichtigung sendet.
- Aktivieren Sie das Kontrollkästchen **Geolokation synchronisieren**, um die geografische Lage von Workstations zwischen den **Dr.Web Servern** zu synchronisieren. Bei aktivierter Option können Sie die folgenden Einstellungen festlegen:
  - **Anlaufsynchronisation**. Hier wird die Anzahl von Workstations ohne geographische Koordinaten angegeben, über die Informationen bei der Herstellung einer Verbindung zwischen **Dr.Web Servern** angefordert werden.

7.2.1.1. Datenverkehr verschlüsseln und komprimieren

Das Antivirus-Netzwerk von **Dr.Web Enterprise Security Suite** bietet die Möglichkeit, den Datenverkehr zwischen dem **Server** und Workstations (**Dr.Web Agents**), zwischen den **Dr.Web Servern** (wenn das Antivirus-Netzwerk aus mehreren Servern besteht) sowie zwischen dem **Server** und **Netzwerk-Installern** zu verschlüsseln. Dieser Modus wird verwendet, damit Benutzerschlüssel, Informationen zur Hardware und Software sowie zu Benutzern des Antivirus-Netzwerks nicht kompromittiert werden.

Das Antivirus-Netzwerk **Dr.Web Enterprise Security Suite** verwendet sichere kryptographische Verschlüsselungsmechanismen und digitale Signaturen, die auf dem asymmetrischen Verschlüsselungsverfahren basieren.

Die Verschlüsselungsrichtlinie wird für jede Komponente des Antivirus-Netzwerks individuell konfiguriert. Die Einstellungen anderer Komponenten müssen dabei auf die Einstellungen des **Servers** abgestimmt werden.

Da das Volumen des Datenverkehrs zwischen den Komponenten (besonders zwischen den **Servern**) sehr groß sein kann, ermöglicht das Antivirus-Netzwerk, diesen Datenverkehr zu komprimieren. Die Komprimierungsrichtlinie sowie die Kompatibilität der Einstellungen zwischen unterschiedlichen Komponenten sind denen zur Verschlüsselungsrichtlinie ähnlich.

Achten Sie beim Konfigurieren der Verschlüsselungs- und Komprimierungseinstellungen darauf, dass die Verschlüsselung und/oder Komprimierung nicht für alle Clients möglich sind (**Dr.Web Antivirus für Android** und **Dr.Web Antivirus für Android MAC OS X** unterstützen weder Verschlüsselung noch Komprimierung). Diese Clients können sich mit dem **Server** nicht verbinden, wenn der Wert **Ja** für die Verschlüsselung und/oder Komprimierung auf dem **Server** festgelegt ist.

So definieren Sie die Komprimierungs- und Verschlüsselungsrichtlinien für Dr.Web Server

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster den Punkt des Verwaltungsmenüs **Dr.Web Server-Konfiguration**.
3. Wählen Sie auf der Registerkarte **Allgemein** in den Dropdown-Listen **Verschlüsselung** und **Komprimierung** eine der folgenden Optionen:
   - **Ja**. Dieser Wert erzwingt die Verschlüsselung (bzw. Komprimierung) des Datenverkehrs für alle Komponenten (dies ist der Standardwert für die Verschlüsselungsoption, wenn kein anderer Wert bei der Installation des **Servers** festgelegt wurde).
   - **Möglich**. Dieser Wert erzwingt die Verschlüsselung (bzw. Komprimierung) des Datenverkehrs für die Komponenten, deren Einstellungen das nicht verbieten.
   - **Nein**. Bei der Auswahl dieses Werts findet keine Verschlüsselung (bzw. Komprimierung) statt (dies ist Standardwert für die Komprimierungsoption, falls kein anderer Wert bei der Installation des **Servers** festgelegt wurde).

Wenn Sie die Einstellungen der Verschlüsselung und Komprimierung auf dem **Server** und in einer anderen Komponente (im **Agent** oder **Netzwerk-Installer**) aufeinander abstimmen, müssen Sie berücksichtigen, dass einige Kombinationen der Einstellungen unzulässig sind, da sie zum Abbruch der Kommunikation zwischen dem **Server** und der Komponente führen können.

Die Tabelle 7-1 gibt Ihnen Übersicht über alle unzulässigen Kombinationen der Einstellungen (**Fehler**) sowie über die Kombinationen, bei denen die Kommunikation zwischen dem **Server** und einer Komponente verschlüsselt/komprimiert (+) bzw. nicht verschlüsselt/nicht komprimiert (–) erfolgt.

Tabelle 7-1: Vereinbarkeit der Einstellungen für die Verschlüsselung und Komprimierung

Einstellungen der Komponente	Einstellung des Servers		
	Ja	Möglich	Nein
Ja	+	+	Fehler
Möglich	+	+	–
Nein	Fehler	–	–

Die Verschlüsselung des Datenverkehrs kann ältere oder leistungsschwache Rechner stark belasten. Wenn keine dringende Notwendigkeit dazu besteht, können Sie keine Verschlüsselung verwenden. Die Verschlüsselung ist auch in großen Netzwerken (mit mehr als 2000 Clients) nicht empfehlenswert.

Achten Sie dabei auf die richtige Reihenfolge beim Deaktivieren der Verschlüsselung: Schalten Sie zuerst den **Server** und Komponenten in den Modus **Möglich** um, indem Sie die unzulässigen Kombinationen **Netzwerk-Installer-Server** und **Agent-Server** vermeiden. Ein Nichteinhalten dieser Regel führt zur Fehlfunktion der Komponente, so dass diese eventuell erneut installiert werden muss.

Die Komprimierung reduziert zwar wesentlich das Datenvolumen, doch wird der Rechner dabei deutlich mehr belastet als bei der Verschlüsselung.

Der Wert **Möglich**, der auf dem **Dr.Web Agent** festgelegt ist, gibt an, dass die Verschlüsselung/ Komprimierung standardmäßig aktiviert ist. Diese Festlegung kann aber durch die Änderung der identischen Einstellungen auf dem **Dr.Web Server** außer Kraft gesetzt werden, ohne dass die festgelegten Einstellungen auf dem **Agent** geändert werden müssen.

7.2.1.2. Datenverbrauch von Workstations begrenzen

Sie können im Antivirus-Netzwerk von **Dr.Web Enterprise Security Suite** die Übertragungsrate, mit der Daten zwischen dem **Server** und **Agents** übertragen werden, begrenzen. Sie können dabei Einschränkungen für die Übertragung von Updates und Installationsdateien von **Agents** separat festlegen.

Sie können den Datenverkehr auf eine der folgenden Weisen beschränken:

1. Beschränkung der gesamten Übertragungsrate für alle Workstations.

   Diese Beschränkung wird im Bereich der **Server**-Konfiguration festgelegt. Wechseln Sie dafür im Hauptmenü des **Verwaltungscenters** zum Punkt **Administrierung** → dann zu **Dr.Web Server-Konfiguration** → **Datenverkehr** → **Updates** oder **Installationen** → **Datenverkehr einschränken**.

2. Individuelle Beschränkung der Übertragungsrate für bestimmte Workstations oder Gruppen von Workstations.

   Diese Beschränkung wird in den Einstellungen der jeweiligen Workstation festgelegt. Wechseln Sie dafür im Hauptmenü des **Verwaltungscenters** zum Punkt **Antivirus-Netzwerk** → und wählen Sie dann in der Liste die gewünschte Workstation oder Gruppe → dann den Punkt **Update-Restriktionen** → **Updates** oder **Installationen** → und dann die Option **Update-Traffic einschränken**.

Einschränkungen für Datenübertragung werden wie folgt vorgenommen:

1. Wenn Sie in den Einstellungen des **Servers** die gesamte Übertragungsrate beschränkt haben, wird der angegebene Wert der gesamten Übertragungsrate bei der Übertragung von Daten vom **Server** auf alle Workstations nicht überschritten. Achten Sie dabei auf das Folgende:

a) Die Übertragungsrate wird trotz der vorhandenen Kapazität der Übertragungskanäle zwischen dem **Server** und Workstations auf alle Workstations gleichmäßig verteilt.

b) Wenn die Kapazität des Übertragungskanals zwischen dem **Server** und einer Workstation weniger als der gemäß dem obigen Punkt **a)** berechnete Durchschnittswert der Übertragungsrate pro Workstation ist, wird die Übertragungsrate für solche Workstation auf die maximale Übertragungsrate vor dieser Workstation eingeschränkt. Die restliche beschränkte Gesamtübertragungsrate wird gemäß dem obigen Punkt **a)** auf alle anderen Workstations gleichmäßig verteilt.

2. Wenn Sie in den Einstellungen einer Gruppe oder Workstation die Übertragungsrate individuell begrenz haben, wird der Wert der festgelegten Übertragungsrate für diese Workstation oder Gruppe nicht überschritten. Für alle anderen Workstations gelten keine Einschränkungen, und Daten werden mit der maximalen Übertragungsrate übertragen.
3. Wenn Sie in den Einstellungen des **Servers** die gesamte Übertragungsrate beschränkt und dabei eine individuelle Übertragungsrate für eine Gruppe oder Workstation festgelegt haben, müssen Sie auf das Folgende achten:

   a) Die Übertragungsrate für die Übertragung von Daten auf eine Gruppe oder Workstation mit einer individuellen Beschränkung überschreitet nicht den Wert, der in den Einstellungen dieser Gruppe oder Workstation festgelegt ist.

   b) Die Übertragungsrate für die Übertragung von Daten auf alle anderen Workstations wird wie folgt berechnet: Die beschränkte Gesamtübertragungsrate nach Abzug des Wertes aus dem obigen Punkt **a)** wird dann gleichmäßig verteilt.

   c) Wenn die Kapazität des Übertragungskanals zwischen dem **Server** und einer Workstation mit keiner individuellen Beschränkung weniger als der gemäß dem obigen Punkt **b)** berechnete Durchschnittswert der Übertragungsrate pro Workstation ist, wird die Übertragungsrate für solche Workstation auf die maximale Übertragungsrate vor dieser Workstation eingeschränkt. Die restliche beschränkte Gesamtübertragungsrate wird gemäß dem obigen Punkt **b)** auf alle anderen Workstations mit keiner individuellen Beschränkung gleichmäßig verteilt.

7.2.2. DNS

Auf der Registerkarte **DNS** werden die Einstellungen für Anfragen an den DNS-Server festgelegt:

- **Timeout für DNS-Anfragen (Sek.)**. Hier wird das Zeitlimit (in Sekunden) für die Auflösung von direkten/inversen DNS-Anfragen festgelegt. Wählen Sie den Wert 0, um die Wartezeit bis zum Ende der Auflösung einer DNS-Anfrage nicht einzuschränken.
- **Anzahl der wiederholten DNS-Anfragen**. Hier wird die maximale Anzahl der DNS-Wiederholungsanfragen bei einer fehlgeschlagenen Auflösung der DNS-Anfrage festgelegt.
- Aktivieren Sie das Kontrollkästchen **Geben Sie den Zeitraum für die Speicherung der Antworten des DNS-Servers ein**, um einen Zeitraum für die Speicherung der Antworten des DNS-Servers im Cache (TTL) festzulegen.
  - **Für positive Antworten (Min.)**. Hier wird der Zeitraum (in Minuten) angegeben, in dem positive Antworten des DNS-Servers im Cache (TTL) behalten werden sollen.
  - **Für negative Antworten (Min.)**. Hier wird der Zeitraum (in Minuten) angegeben, in dem negative Antworten des DNS-Servers im Cache (TTL) behalten werden sollen.
- **DNS-Server**. Hier wird die Liste der DNS-Server zusammengestellt, welche die standardmäßige Systemliste ersetzen soll.
- **DNS-Domänen**. Hier wird die Liste der DNS-Domänen zusammengestellt, welche die standardmäßige Systemliste ersetzen soll.

7.2.3. Statistik

Auf der Registerkarte **Statistik** können Sie angeben, welche Statistiken in die Protokolldatei und Datenbank des **Servers** aufgenommen werden sollen.

Um bestimmte Informationstypen aufzeichnen und in die Datenbank aufnehmen zu lassen, aktivieren Sie die entsprechenden Kontrollkästchen:

- **Status der Quarantäne**. Diese Option ermöglicht die Überwachung des Status der **Quarantäne** auf Workstations und Aufzeichnung dieser Informationen in der Datenbank.
- **Informationen zur Hardware und Software**. Diese Option ermöglicht die Überwachung der Hardware und Software von Workstations sowie Aufzeichnung dieser Informationen in der Datenbank.
- **Liste der Module der Workstations**. Diese Option ermöglicht die Überwachung der Liste der **Antivirus**-Module auf Workstations zu überwachen sowie Aufzeichnung dieser Informationen in der Datenbank.
- **Liste der installierten Komponenten**. Diese Option ermöglicht die Überwachung der auf der Workstation installierten **Antivirus**-Komponenten (darunter **Scanner**, **Wächter** usw.) sowie Aufzeichnung dieser Informationen in der Datenbank.
- **Sitzungen der Benutzer von Workstations**. Mit dieser Option lassen Sie Sitzungen der Benutzer von Workstations überwachen und Anmeldenamen der Benutzer, die sich am Rechner mit dem installierten **Agent** anmeldeten, in die Datenbank aufnehmen.
- **Start/Beenden der Komponenten**. Mit dieser Option lassen Sie den Start und das Beenden der auf der Workstation installierten **Antivirus**-Komponenten (darunter **Scanner**, **Wächter** usw.) überwachen sowie diese Informationen in die Datenbank aufnehmen.
- **Erkannte Sicherheitsbedrohungen**. Diese Option ermöglicht die Überwachung von auf Workstations erkannten Bedrohungen sowie Aufzeichnung dieser Informationen in der Datenbank.

  Wenn das Kontrollkästchen **Erkannte Sicherheitsbedrohungen** aktiviert ist, können Sie statistische Informationen zu erkannten Bedrohungen an Doctor Web senden.

  Um Statistiken zu erkannten Sicherheitsbedrohungen an **Doctor Web** zu versenden, aktivierten Sie das Kontrollkästchen **Statistik an Doctor Web einsenden**. Die folgenden Felder werden dabei verfügbar:

  - **Zeitabstand**. Hier wird der Sendeintervall (in Minuten) angegeben.
  - **Identifikator**. Hier wird der MD5-Schlüssel (befindet sich in der Konfigurationsdatei des **Servers**) angegeben.

  Zum Versand von Statistiken reicht es aus, nur das Feld **Zeitabstand** auszufüllen.

- **Scan-Fehler**. Diese Option ermöglicht die Überwachung eventueller Fehler beim Scannen von Workstations sowie Aufzeichnung dieser Informationen in der Datenbank.
- **Scan-Statistik**. Diese Option ermöglicht die Überwachung der Scan-Ergebnisse auf Workstations sowie Aufzeichnung dieser Informationen in der Datenbank.
- **Installationen des Agents**. Diese Option ermöglicht das Sammeln der Informationen über die Installationen von **Agents** sowie Aufzeichnung dieser Daten in der Datenbank.
- **Verlauf der Aufgabenausführung**. Diese Option ermöglicht die Überwachung der Ergebnisse der Aufgaben, die auf Workstations durchgeführten wurden, sowie Aufzeichnung dieser Informationen in der Datenbank.
- **Status der Workstations**. Diese Option ermöglicht die Überwachung von Änderungen am Status von Workstations sowie Aufzeichnung dieser Informationen in der Datenbank.
  - **Status der Virendatenbanken**. Diese Option ermöglicht die Überwachung des Status von Virendatenbanken (darunter ihr Anzahl und eventuelle Änderungen) auf Workstations sowie Aufzeichnung dieser Informationen in der Datenbank. Das Kontrollkästchen ist auswählbar, wenn das Kontrollkästchen **Status der Workstations** aktiviert ist.

So lassen Sie statistische Informationen anzeigen

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie in der hierarchischen Liste die gewünschte Workstation oder Gruppe.
3. Öffnen Sie im Verwaltungsmenü den entsprechenden Bereich (s. Tabelle unten).

Diese statistischen Daten werden im Abschnitt Statistik zu einer Workstation anzeigen detailliert beschrieben.

In der Tabelle unten finden Sie Informationen dafür, wie die Kontrollkästchen im Bereich **Statistik** in den Einstellungen des **Servers** und die Punkte des Verwaltungsmenüs auf der Seite **Antivirus-Netzwerk** miteinander übereinstimmen.

Wenn einige Kontrollkästchen auf der Registerkarte **Statistik** deaktiviert sind, werden die entsprechenden Punkte im Verwaltungsmenü ausgeblendet.

Tabelle 7-2: Korrespondenz zwischen den Einstellungen des Servers und Punkten des Verwaltungsmenüs

Einstellung des Servers	Menüpunkte
Status der Quarantäne	Allgemein→ Quarantäne Konfiguration → Windows → Dr.Web Agent → Remotesteuerung der Quarantäne zulassen
Informationen zur Hardware und Software	Allgemein → Hardware und Software Allgemein → Vergleich der Hardware und Software
Liste der Module der Workstations	Statistik → Module
Liste der installierten Komponenten	Allgemein → Installierte Komponenten
Sitzungen der Benutzer von Workstations	Allgemein → Benutzersitzungen
Start/Beenden der Komponenten	Statistik → Start/Herunterfahren
Erkannte Sicherheitsbedrohungen	Statistik → Bedrohungen Statistik → Statistiken zu Bedrohungen
Scan-Fehler	Statistik → Fehler
Scan-Statistik	Statistik → Scan-Statistik Tabellen → Gesamtstatistik
Installationen des Agents	Statistik → Alle Netzwerkinstallationen
Verlauf der Aufgabenausführung	Statistik → Aufgaben Statistik → Virendatenbanken
Status der Workstations	Statistik → Status Statistik → Virendatenbanken
Status der Virendatenbanken	Statistik → Virendatenbanken

7.2.4. Sicherheit

Auf der Registerkarte **Sicherheit** können Sie Einschränkungen für Netzwerkadressen festlegen, über die **Agents**, Netzwerk-Installer und andere (benachbarte) **Dr.Web Server** auf den **Server** zugreifen.

Das Audit-Protokoll des **Servers** wird über die folgenden Kontrollkästchen verwaltet:

- **Vorgänge des Administrators überwachen**. Diese Option ermöglicht, alle Aktionen, die der Administrator im **Verwaltungscenter** vornimmt, zu protokollieren sowie diese Informationen in der Datenbank aufzuzeichnen.
- **Interne Server-Vorgänge überwachen** Diese Option ermöglicht, alle internen Vorgänge des **Dr.Web Servers** zu protokollieren und diese Informationen in der Datenbank aufzuzeichnen.
- **Web API-Vorgänge überwachen**. Diese Option ermöglicht, alle XML-API-Vorgänge zu protokollieren und diese Informationen in der Datenbank aufzuzeichnen.

Um das Überwachungsprotokoll anzuzeigen, wählen Sie im Hauptmenü **Administrierung** den Punkt **Audit-Log**.

Die Registerkarte **Sicherheit** enthält zusätzliche Registerkarten, auf denen Sie Einschränkungen für einzelne Verbindungstypen festlegen können.

- **Agents**. Hier werden Einschränkungen für IP-Adressen angegeben, über die **Dr.Web Agents** auf den **Server** zugreifen können.
- **Installationsprogramme**. Hier werden Einschränkungen für IP-Adressen angegeben, über welche die Installationsprogramme von **Dr.Web Agents** auf den **Server** zugreifen können.
- **Nachbarn**. Hier werden Einschränkungen für IP-Adressen angegeben, über die benachbarte **Dr.Web Server** auf den **Server** zugreifen können.
- **Suchdienst**. Hier werden Einschränkungen für IP-Adressen angegeben, von denen der Server-Suchdienst Broadcastanforderungen empfangen kann.

So legen Sie Zugriffseinschränkungen für einen Verbindungstyp fest

1. Wechseln Sie zur benötigten Registerkarte (**Agenten**, **Installationen**, **Nachbarn** oder **Suchdienst**).
2. Um alle Verbindungen zu erlauben, deaktivieren Sie das Kontrollkästchen **Diese Zugriffssteuerungsliste verwenden**.
3. Um eine Liste der zugelassenen bzw. verbotenen Adressen zusammenzustellen, aktivieren Sie das Kontrollkästchen **Diese Zugriffssteuerungsliste verwenden**.
4. Um eine TCP-Adresse zuzulassen, fügen Sie diese der Liste **TCP: Erlaubt** oder **TCPv6: Erlaubt** hinzu.
5. Um eine TCP-Adresse zu verbieten, fügen Sie diese der Liste **TCP: Verboten** oder **TCPv6: Verboten** hinzu.

So bearbeiten Sie die Liste von Adressen

1. Geben Sie ins entsprechende Feld die gewünschte Netzwerkadresse ein und klicken Sie dann auf **Speichern**.
2. Um ein neues Feld hinzuzufügen, klicken Sie im entsprechenden Bereich auf die Schaltfläche .
3. Um ein Feld zu löschen, klicken Sie auf .

   Die Netzwerkadresse muss wie folgt angegeben werden: *<IP-Adresse>*/[*<Präfix>*].

Listen für TCPv6-Adressen werden nur dann eingeblendet, wenn der Rechner über die IPv6-Schnittstelle verfügt.

Beispiel für einen Präfix:

1. Das Präfix 24 steht für Netzwerke mit einer Subnetzmaske: `255.255.255.0`

   Beinhaltet 254 Adressen

   Hostadressen in diesen Netzwerken sehen so aus: `195.136.12.*`

2. Das Präfix 8 steht für Netzwerke mit einer Subnetzmaske: `255.0.0.0`

   Beinhaltet bis zu 16387064 Adressen (256*256*256)

   Hostadressen in diesen Netzwerken sehen so aus: `125.*.*.*`

Adressen, die keiner der Listen hinzugefügt wurden, werden je nach dem, ob das Kontrollkästchen **Priorität des Verbots** aktiviert ist, zugelassen oder verboten. Wenn das Kontrollkästchen aktiviert ist, hat die Liste **Verboten** Vorrang gegenüber der Liste **Erlaubt**. Adressen, die keiner Liste bzw. beiden Listen hinzugefügt wurden, werden nicht zugelassen. Erlaubt sind nur Adressen, die der Liste **Erlaubt** hinzugefügt sind und nicht in der Liste **Verboten** vorhanden sind.

7.2.5. Cache

Auf der Registerkarte **Cache** werden die Einstellungen für das Löschen vom Server-Cache festgelegt:

- **Cache-Bereinigungsintervall**. Hier wird das Zeitintervall angegeben, nach dessen Ablauf der Cache vollständig gelöscht werden soll.
- **Dateien in Quarantäne**. Hier wird das Zeitintervall angegeben, nach dessen Ablauf Dateien in der **Quarantäne** auf dem **Server** gelöscht werden sollen.
- **Installationspakete**. Hier wird das Zeitintervall angegeben, nach dessen Ablauf persönliche Installationspakete gelöscht werden sollen.
- **Repository-Dateien**. Hier wird das Zeitintervall angegeben, nach dessen Ablauf Dateien im Repository gelöscht werden sollen.

  Achten Sie bei der Angabe von numerischen Werten auf die Zeiteinheiten in den Dropdown-Listen.

7.2.6. Datenbank

Auf der Registerkarte **Datenbank** können Sie ein Datenbankmanagementsystem für den **Dr.Web Server** auswählen.

Zur Anzeige der Struktur der Datenbank des **Dr.Web Servers** können Sie das SQL-Skript `init.sql` verwenden, das sich im Unterverzeichnis `etc` vom Installationsverzeichnis des **Dr.Web Servers** befindet.

1. Wählen Sie in der Dropdown-Liste **Datenbank** einen Datenbanktyp aus:
   - **IntDB** – ist eine eingebettete SQLite2-Datenbank (Komponente des **Dr.Web Servers**).
   - **ODBC** – für eine externe Datenbank, auf die über die ODBC-Verbindung zugegriffen wird.
   - **Oracle** – ist eine externe Datenbank für alle Betriebssysteme, FreeBSD ausgenommen.

Bei der Verwendung einer externen **Oracle** -Datenbank, auf die über die ODBC-Verbindung zugegriffen wird, müssen Sie die aktuellste Version des mitgelieferten ODBC-Treibers installieren. Sie sollten keine Microsoft ODBC-Treiber für Oracle verwenden.

   - **PostgreSQL** – ist eine externe Datenbank.

- **SQLite3** – ist eine eingebettete Datenbank (Komponente des **Dr.Web Servers**). Diese Option ist bei der Verwendung einer eingebetteten Datenbank empfehlenswert.

2. Legen Sie die benötigten Einstellungen für die Datenbank fest:
   - Für eingebettete Datenbanken könne Sie im Feld **Dateiname** den vollständigen Pfad zur Datenbankdatei angeben und die Cachegröße sowie den Modus für die Datenbankprotokollierung festlegen.
   - Die Einstellungen für externe Datenbanken werden im Dokument **Anhänge** im Anhang B. Einstellungen des DBMS. Einstellungen für DBMS-spezifische Treiber beschrieben.
3. Übernehmen Sie die Einstellungen mit einem Klick auf **Speichern**.

Die Distribution des **Dr.Web Servers** enthält integrierte Clients für alle unterstützten DBMS. Aus diesem Grund müssen Sie das Folgende berücksichtigen:

- Wenn Sie die zusammen mit dem **Dr.Web Server** gelieferten integrierten DBMS-Clients verwenden wollen, müssen Sie bei der Installation (Aktualisierung) des **Servers** in den Einstellungen des Installationsprogramms den Punkt **Benutzerdefiniert** auswählen und im nächsten Fenster überprüfen, dass die Installation des entsprechenden integrierten DBMS-Clients im Bereich **Database support** erlaubt ist.
- Wenn Sie auf externe Datenbanken über die ODBC-Verbindung zugreifen wollen, müssen Sie bei der Installation (Aktualisierung) des **Servers** in den Einstellungen des Installationsprogramms den Punkt **Benutzerdefiniert** auswählen und im nächsten Fenster im Bereich **Database support** die Installation des entsprechenden integrierten DBMS-Clients deaktivieren.
  Anderenfalls kann auf die Datenbank über die ODBC-Verbindung aufgrund eventueller Probleme durch inkompatible Bibliotheken nicht zugegriffen werden.

Das Installationsprogramm des **Servers** unterstützt die benutzerdefinierte Installation. Um einzelne Komponenten, wie etwa DBMS-spezifische Treiber, hinzuzufügen bzw. zu löschen, starten Sie das Installationsprogramm des **Servers** und wählen Sie **Ändern** aus.

Standardmäßig wird ein eingebettetes DBMS verwendet. Im diesem Modus wird der **Server** ziemlich stark belastet. Wenn Ihr Antivirus-Netzwerk sehr groß ist, sollten Sie sich für ein externes DBMS entscheiden. Im Dokument **Anhänge** im Abschnitt DBMS von Dr.Web Enterprise Security Suite wechseln wird beschrieben, wie Sie den Datenbanktyp ändern können.

Damit eine eingebettete Datenbank eingesetzt werden kann, dürfen mit dem **Server** nicht mehr als 200-300 Workstations verbunden werden. Wenn der Rechner, auf dem **Dr.Web Server** installiert ist, über ausreichend leistungsfähige Hardware verfügt und einer geringen Auslastung durch andere Prozesse ausgesetzt ist, können dann bis zu 1000 Workstations verbunden werden.

Anderenfalls sollte eine externe Datenbank verwendet werden.

Bei der Verwendung einer externen Datenbank und bei der Verbindung mit dem **Server** von mehr als 10000 Workstations ist es empfehlenswert, mindestens die folgenden Anforderungen einzuhalten:

- Prozessor mit Taktfrequenz von 3 GHz
- Mindestens 4 GB freier Hauptspeicher für **Dr.Web Server** und mindestens 8 GB für Datenbankserver
- Ein UNIX-ähnliches Betriebssystem

Sie können die vom **Dr.Web Server** verwendete Datenbank aufräumen: Sie können Einträge über Ereignisse sowie Informationen zu Workstations, die keine Verbindung mit dem **Server** innerhalb von einem bestimmten Zeitraum nicht hergestellt haben, löschen. Um die Datenbank auf dieser Weise aufzuräumen, wechseln Sie zum Server-Zeitplan und planen Sie die benötigte Aufgabe.

7.2.7. Proxy

Auf der Registerkarte **Proxy** werden die Proxy-Server-Einstellungen festgelegt.

Aktivieren Sie das Kontrollkästchen **Proxyserver verwenden**, damit Verbindungen mit dem **Dr.Web Server** über einen Proxy-Server hergestellt werden können. Nach der Aktivierung können Sie die folgenden Einstellungen festlegen:

- **Proxyserver**. Hier wird die IP-Adresse bzw. der DNS-Name des Proxy-Servers angegeben.
- Damit eine Autorisierungsmethode zum Zugriff auf den Proxy-Server verwendet wird, aktivieren Sie das Kontrollkästchen **Autorisierung verwenden** und legen Sie die folgenden Einstellungen fest:
  - Füllen Sie die Felder **Proxyserver-Benutzer** und **Passwort des Proxyserver-Benutzers** aus.
  - Wählen Sie eine der folgenden Autorisierungsmethoden:

Option		Erläuterung
Beliebige unterstützte Methode		Eine beliebige von dem Proxy-Server unterstützte Autorisierungsmethode wird verwendet. Wenn der Proxy-Server mehrere Autorisierungsmethoden unterstützt, wird die sicherste Option verwendet.
Beliebige sichere unterstützte Methode		Eine beliebige sichere Autorisierungsmethode, die vom Proxy-Server unterstützt wird, wird verwendet. In diesem Modus ist keine Basic-Autorisierung möglich. Wenn der Proxy-Server mehrere Autorisierungsmethoden unterstützt, wird die sicherste Option verwendet.
Unten angegebene Methoden:	Basic-Autorisierung	Die Basic-Autorisierung wird verwendet. Die Methode ist nicht empfehlenswert, da bei dieser Methode Anmeldedaten unverschlüsselt vermittelt werden.
	Digest-Autorisierung	Die Digest-Autorisierung wird verwendet. Dabei handelt es sich um eine kryptographische Autorisierungsmethode.
	NTLM-Autorisierung	Die NTLM-Autorisierung wird verwendet. Dabei handelt es sich um eine kryptographische Autorisierungsmethode, bei der das NTLM-Protokoll von Microsoft verwendet wird.
	GSS-Negotiate-Autorisierung	Die GSS-Negotiate-Autorisierung wird verwendet. Dabei handelt es sich um eine kryptographische Autorisierungsmethode.

7.2.8. Transport

Auf der Registerkarte **Transport** können Sie die Einstellungen der Transportprotokolle, die vom **Server** zur Kommunikation mit Clients verwendet wird, festlegen.

Im Bereich für TCP/IP werden die Parameter für die TCP/IP-Verbindung mit dem **Server** festgelegt:

- Geben Sie in den Feldern **Adresse** und **Port** die IP-Adresse und die Portnummer der Netzwerkschnittstelle an, an die dieses Transportprotokoll gebunden wird. Der **Server** wird an der festgelegten Netzwerkschnittstelle lauschen, um mit den auf Workstations installierten **Agents** zu kommunizieren.
- Geben Sie im Feld **Name** den Namen des **Dr.Web Servers** an. Wenn kein Name festgelegt wurde, wird der auf der Registerkarte **Allgemein** angegebene Name verwendet (s. oben, wenn kein Name auf dieser Registerkarte angegeben ist, wird der Name des Rechners verwendet). Wenn der Name für das Protokoll nicht mit dem auf der Registerkarte **Allgemein** angegebenen Namen übereinstimmt, wird der Name aus der Protokollbeschreibung verwendet. Diesen Name verwendet der Suchdienst, damit **Agents** den **Server** finden können.
- Aktivieren Sie das Kontrollkästchen **Suche**, um den **Server**-Suchdienst zu aktivieren.
- Aktivieren Sie das Kontrollkästchen **Multicasting**, um den Modus *Multicast over UDP* bei der Suche nach dem **Server** zu verwenden.
- Geben Sie im Feld **Multicast-Gruppe** die IP-Adresse der Multicast-Gruppe an, in welcher der **Server** registriert wurde. Diese Gruppe wird zur Kommunikation mit den **Agents** und **Netzwerk-Installern** bei der Suche nach aktiven **Dr.Web Servern** verwendet. Wenn Sie dieses Feld leer lassen, wird die Gruppe `231.0.0.1` standardmäßig verwendet.

- Nur bei UNIX-artigen Betriebssystemen: Geben Sie im Feld **Pfad** den Pfad zum Verbindungssocket, z. B. für den **Agent**, an.

Mehr dazu finden Sie im Abschnitt Netzwerkverbindungen konfigurieren.

Diese Parameter müssen im Format einer Netzwerkadresse angegeben werden. Die erlaubten Schreibweisen finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation der Netzwerkadresse.

7.2.9. Module

Auf der Registerkarte **Module** können Sie die Einstellungen für die Kommunikation zwischen dem **Dr.Web Server** und den anderen Komponenten von **Dr.Web Enterprise Security Suite** festlegen:

- Aktivieren Sie das Kontrollkästchen **Browser-Erweiterung für Dr.Web Sicherheitscenter**, um die **Browser-Erweiterung für Dr.Web Sicherheitscenter** zur Verwaltung des **Servers** und Antivirus-Netzwerks über das **Verwaltungscenter** zu verwenden.

Wenn das Kontrollkästchen **Browser-Erweiterung für Dr.Web Sicherheitscenter** deaktiviert ist, wird das **Dr.Web Sicherheitscenter** nach dem Neustart des **Dr.Web Servers** nicht verfügbar. Sie können aber den **Server** und das Antivirus-Netzwerk mithilfe des Dienstprogramms zur Ferndiagnose steuern, vorausgesetzt, dass das Kontrollkästchen **Browser-Erweiterung für Dr.Web Server FrontDoor** aktiviert ist.

- Aktivieren Sie das Kontrollkästchen **Browser-Erweiterung für Dr.Web Server FrontDoor**, um das **Browser-Erweiterung für Dr.Web Server FrontDoor** verwenden zu können. Diese Erweiterung ermöglicht Ihnen, das Programm zur Ferndiagnose des **Servers** zu verwenden (s. auch den Punkt Fernzugriff auf den Dr.Web Server).
- Aktivieren Sie das Kontrollkästchen **Protokoll von Dr.Web Agent**, um das Protokoll für die Kommunikation zwischen dem **Server** und **Dr.Web Agents** zu aktivieren.
- Aktivieren Sie das Kontrollkästchen **Protokoll von Microsoft NAP Health Validator**, um das Protokoll für die Kommunikation zwischen dem **Server** und der Windows-Systemintegritätsprüfung **NAP Validator** zu aktivieren.
- Aktivieren Sie das Kontrollkästchen **Protokoll des Installers von Dr.Web Agent**, um das Protokoll für die Kommunikation zwischen dem **Server** und Installationsprogrammen von **Dr.Web Agents** zu aktivieren.
- Aktivieren Sie das Kontrollkästchen **Protokoll des Clusters von Dr.Web Servern**, um das Protokoll für die Kommunikation zwischen den **Servern** innerhalb eines Clustersystems zu aktivieren.
- Aktivieren Sie das Kontrollkästchen **Protokoll von Dr.Web Server**, um das Protokoll für die Kommunikation zwischen dem **Dr.Web Server** und anderen **Dr.Web Servern** zu aktivieren. Dieses Protokoll ist standardmäßig deaktiviert. Wenn Ihr Netzwerk aus mehreren Servern besteht (s. den Abschnitt Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern), aktivieren Sie dieses Protokoll, indem Sie das Kontrollkästchen **Protokoll von Dr.Web Server** aktivieren.

7.2.10. Cluster

Auf der Registerkarte **Cluster** können Sie die Einstellungen für den Cluster von **Dr.Web Servern** festlegen. Dadurch ist der Datenaustausch möglich, wenn das Antivirus-Netzwerk aus mehreren Servern besteht (s. dazu den Abschnitt Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern).

Um den Cluster zu verwenden, legen Sie die folgenden Einstellungen fest:

- **Multicast-Gruppe**. Hier wird die IP-Adresse der Multicast-Gruppe angegeben, über die der Datenaustausch zwischen den **Servern** stattfinden soll.

- **Port**. Hier wird die Portnummer der Netzwerkschnittstelle angegeben, an die das Transportprotokoll gebunden wird, damit Daten an die Multicast-Gruppe gesendet werden können.
- **Benutzeroberfläche**. Hier wird die IP-Adresse der Netzwerkschnittstelle angegeben, an die das Transportprotokoll, über das Informationen an die Multicast-Gruppe gesendet werden, gebunden wird.

7.2.11. Standort

Auf der Registerkarte **Standort** können Sie zusätzliche Informationen über den Standort des Rechners, auf dem die Software des **Dr.Web Servers** installiert ist, angeben.

Darüber hinaus wird hier die Lage des **Servers** auf der geographischen Karte angezeigt.

So lassen Sie die Lage des Servers auf der Karte anzeigen

1. Geben Sie in den Feldern **Breite** und **Länge** die geographischen Koordinaten des **Servers** in Dezimalgrad (Decimal Degrees) an.
2. Klicken Sie auf **Speichern**, um die eingegebenen Daten in der Konfigurationsdatei des **Servers** zu speichern.

   Zur Anzeige der Karte ist kein Neustart des **Servers** erforderlich. Damit aber die geänderten geografischen Koordinaten wirksam werden, muss der **Server** neu gestartet werden.
3. Auf der Registerkarte **Standort** wird die Vorschau von OpenStreetMaps mit der Markierung des festgelegten Standorts angezeigt.

   Wenn die Vorschau nicht geladen werden kann, erscheint der Text **Auf der Karte anzeigen**.
4. Um die Karte in voller Größe anzeigen zu lassen, klicken Sie auf die Vorschau oder den Text **Auf der Karte anzeigen**.

7.2.12. Herunterladen

Auf der Registerkarte **Herunterladen** können Sie die Einstellungen des **Servers** festlegen, die beim Generieren der Installationsdateien des **Agents** verwendet werden. Anhand dieser Einstellungen stellt dann das Installationsprogramm des **Agents** eine Verbindung mit dem **Server** her:

- **Server** – IP-Adresse oder DNS-Name des **Servers**.

  Wenn die Adresse des **Servers** nicht festgelegt ist, wird der vom Betriebssystem zurückgegebene Name des Rechners verwendet.
- **Port**. Hier wird die Portnummer angegeben, die vom Installationsprogramm des **Agents** zur Herstellung einer Verbindung mit dem **Server** verwendet wird.

  Wenn keine Portnummer festgelegt ist, wird der Port 2193 verwendet (diese Einstellung kann im **Verwaltungscenter** im Bereich **Administrierung** → **Dr.Web Server-Konfiguration** → auf der Registerkarte **Transport** individuell angepasst werden).

Die Einstellungen des Bereichs **Herunterladen** werden in der Konfigurationsdatei `download.conf` gespeichert (s. dazu das Dokument **Anhänge**, den Anhang G3. Konfigurationsdatei download.conf).

7.2.13. Gruppen-Updates

Auf der Registerkarte **Gruppen-Updates** können Sie festlegen, wie Gruppen-Updates an die Workstations über das Multicast-Protokoll übertragen werden können.

Damit Updates an die Workstations übertragen werden können, aktivieren Sie das Kontrollkästchen **Gruppen-Updates aktivieren**. Achtes Sie dabei auf das Folgende:

- Wenn die Gruppen-Updates deaktiviert sind, werden alle Workstations nur über das TCP-Protokoll aktualisiert.
- Wenn die Gruppen-Updates aktiviert sind, werden alle Workstations, die mit diesem **Server** verbunden sind, in zwei Schritten aktualisiert:
  1. Aktualisierung über das Multicast-Protokoll.
  2. Standardmäßige Aktualisierung über das TCP-Protokoll.

Zum Konfigurieren der Gruppen-Updates werden die folgenden Einstellungen verwendet:

- **Größe des UDP-Datagrammes (Bytes)**. Hier wird die Größe der UDP-Datagramme (in Bytes) angegeben, die vom Multicast-Protokoll verwendet werden.

  Zulässig sind die Werte von 512 bis 8192. Zur Vermeidung der Fragmentierung sollte der Wert geringer als der MTU-Wert (maximale Übertragungseinheit) des verwendeten Netzwerks sein.

- **Dateiübertragungszeit (ms)**. Hier wird der Zeitraum angegeben, in dem eine Update-Datei übertragen werden soll. Abschließend sendet der **Server** die nächste Datei.

  Alle Dateien, die bei der Aktualisierung über das Multicast- Protokoll nicht übertragen wurden, werden bei der standardmäßigen Aktualisierung über das TCP-Protokoll übermittelt.

- **Dauer von Gruppen-Updates (ms)**. Hier wird die Dauer der Aktualisierung über das Multicast-Protokoll angegeben.

  Alle Dateien, die bei der Aktualisierung über das Multicast- Protokoll nicht übertragen wurden, werden bei der standardmäßigen Aktualisierung über das TCP-Protokoll übermittelt.

- **Zeitintervall für Paketübertragung (ms)**. Hier wird das Zeitintervall angegeben, mit dem Pakete an eine Multicast-Gruppe gesendet werden sollen.

  Ein geringes Zeitintervall kann erhebliche Verluste in der Paketübertragung verursachen und das Netzwerk überlasten. Ändern Sie diesen Wert nur bei dringendem Bedarf.

- **Zeitintervall zwischen den Anforderungen für wiederholte Übertragung (ms)**. Hier wird das Zeitintervall angegeben, mit dem die **Agents** Anforderungen für die erneute Übertragung verlorener Pakete senden sollen.

  Dr.Web Server speichert diese Anforderungen und leitet dann die verlorenen Blöcke weiter.

- **Zeitintervall für die "Stille" auf der Linie (ms)**. Hier wird das Ruheintervall angegeben: Wenn eine Datei vorzeitig übertragen wurde und die **Agents** innerhalb dieses Ruheintervalls keine Anforderungen für die erneute Übertragung verlorener Pakete senden, nimmt der **Dr.Web Server** an, dass alle **Agents** die gesendete Update-Datei erhalten haben, und sendet abschließend die nächste Datei.
- **Zeitintervall fürs Sammeln von Anforderungen der erneuten Übertragung (ms)**. Hier wird das Zeitintervall angegeben, in dem der **Server** Anforderungen der **Agents** für die erneute Übertragung verlorener Pakete sammeln soll.

  Agents senden Anforderungen für die erneute Übertragung verlorener Pakete. Der **Server** sammelt diese Anforderungen innerhalb des festgelegten Zeitintervalls und leitet dann die verlorenen Blöcke weiter.

Um eine Liste von Multicast-Gruppen, über die Gruppen-Updates übertragen werden, zu erstellen, legen Sie im Bereich **Multicast-Gruppen** die folgenden Einstellungen fest:

- **Multicast-Gruppe**. Hier wird die IP-Adresse der Multicast-Gruppe angegeben, über die Workstations Gruppen-Updates erhalten sollen.
- **Port**. Hier wird die Portnummer der Netzwerkschnittstelle des **Dr.Web Servers** angegeben, an die das Multicast-Transportprotokoll gebunden wird, damit Updates übertragen werden können.

Für Gruppen-Updates muss ein beliebiger freier Port angegeben werden. Er darf aber nicht mit dem Port, der für das Transportprotokoll in den Einstellungen des **Servers** festgelegt wurde, identisch sein.

- **Benutzeroberfläche**. Hier wird die IP-Adresse der Netzwerkschnittstelle des **Dr.Web Servers** angegeben, an die das Multicast-Transportprotokoll gebunden wird, damit Updates übertragen werden können.

  In jeder Zeile wird nur eine Multicast-Gruppe konfiguriert. Um eine weitere Multicast-Gruppe hinzuzufügen, klicken Sie auf .

Wenn Sie mehrere Multicast-Gruppen konfigurieren wollen, beachten Sie das Folgende:

- Für alle **Dr.Web Server**, die Gruppen-Updates versenden sollen, müssen verschiedene Multicast-Gruppen festgelegt werden.
- Bei allen **Dr.Web Servern**, die Gruppen-Updates versenden sollen, müssen die Felder **Benutzeroberfläche** und **Port** nicht identisch festgelegt werden.
- Wenn mehrere Multicast-Gruppen verwendet werden, darf jede Workstation des Antivirus-Netzwerks nur einer Multicast-Gruppe gehören.

7.2.14. Lizenzen

Auf der Registerkarte **Lizenzen** können Sie die Einstellungen für die Verteilung von Lizenzen an die **Dr.Web Server** festlegen:

- **Laufzeit vergebener Lizenzen**. Hier wird der Zeitraum angegeben, für den Lizenzen aus dem Schlüssel des **Servers** verteilt werden sollen. Diese Option wird verwendet, wenn dieser **Server** Lizenzen an benachbarte **Server** verteilt.
- **Zeitraum für Verlängerung von erhaltenen Lizenzen**. Hier wird der Zeitraum bis zum Ablauf der Lizenz angegeben, ab dem dieser **Server** die Verlängerung der von dem benachbarten **Server** erhaltenen Lizenz initiiert. Diese Option wird verwendet, wenn der **Server** Lizenzen von benachbarten **Servern** verteilt bekommt.
- **Synchronisationszeitraum der Lizenzen**. Hier wird das Zeitintervall angegeben, mit dem Informationen zu vergebenen Lizenzen zwischen den **Servern** synchronisiert werden sollen.

Detaillierte Informationen über die Verteilung von Lizenzen auf **Server** finden Sie unter Lizenzmanager.

7.3. Fernzugriff auf den Dr.Web Server

Um das Dienstprogramm zur Ferndiagnose des **Servers** verwenden zu können, aktivieren Sie die **Browser-Erweiterung für Dr.Web Server FrontDoor**. Aktivieren Sie dafür im Bereich **Dr.Web Server-Konfiguration** auf der Registerkarte Module das Kontrollkästchen **Browser-Erweiterung für Dr.Web Server FrontDoor**.

Um das Dienstprogramm zur Ferndiagnose des **Servers** verwenden zu können, muss der Administrator über die Berechtigung **Zusatzoptionen nutzen** verfügen. Anderenfalls ist der Zugriff auf den **Server** über das Dienstprogramm zur Ferndiagnose nicht möglich.

So konfigurieren Sie die Verbindungseinstellungen des Dienstprogramms zur Ferndiagnose des Servers

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Fernzugriff auf Dr.Web Server**.
2. Legen Sie die folgenden Einstellungen fest:
   - **SSL-Zertifikat**. Hier wird die Datei des SSL-Zertifikats angegeben, das bei der Herstellung der Verbindung überprüft wird. Die Dropdown-Liste enthält alle im Verzeichnis des **Servers** verfügbaren Zertifikate.
   - **Privater SSL-Schlüssel**. Hier wird die Datei des privaten SSL-Schlüssels angegeben, der bei der Herstellung der Verbindung überprüft wird Die Dropdown-Liste enthält alle im Verzeichnis des **Servers** verfügbaren privaten SSL-Schlüssel.
   - **Adresse**. Hier wird die Adresse angegeben, die bei der Herstellung der Verbindung mit dem Dienstprogramm zur Ferndiagnose des **Servers** verwendet wird.
   - **Port**. Hier wird der Port zur Verbindung mit dem Dienstprogramm zur Ferndiagnose des **Servers** angegeben. Der Standardport ist 10101.
3. Klicken Sie auf **Speichern**.

Die Verwendung der Konsolenversion des Dienstprogramms zur Ferndiagnose des **Servers** wird im Dokument **Anhänge** unter H9. Dienstprogramm zur Ferndiagnose des Dr.Web Servers detailliert beschrieben.

7.4. Zeitplan des Dr.Web Servers konfigurieren

So bearbeiten Sie den Zeitplan des Dr.Web Servers

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Dr.Web Server-Aufgabenplaner**. Die Liste von Aufgaben des **Servers** wird angezeigt.
2. Zur Verwaltung des Zeitplans werden die folgenden Elemente in der Symbolleiste verwendet:

   a) Allgemeine Elemente der Symbolleiste dienen zur Erstellung neuer Aufgaben und zur allgemeinen Verwaltung des Zeitplans. Diese Tools sind jederzeit auf der Symbolleiste verfügbar.

Aufgabe erstellen – fügt eine neue Aufgabe hinzu. Mehr Information zu dieser Aktion finden Sie unten, im Unterabschnitt Aufgaben-Editor.

Einstellungen aus diesem Bereich in die Datei exportieren – exportiert den Zeitplan in eine Datei im speziellen Format.

Einstellungen aus der Datei in diesen Bereich importieren – importiert den Zeitplan aus einer Datei im speziellen Format.

   b) Um bereits bestehende Aufgaben zu verwalten, aktivieren Sie die Kontrollkästchen neben den gewünschten Aufgaben oder in der Überschrift der Tabelle, falls alle Aufgaben in der Liste ausgewählt werden müssen. Elemente zur Verwaltung von ausgewählten Aufgaben werden dabei auf der Symbolleiste verfügbar.

Tabelle 7-3: Symbolleistenelemente zur Verwaltung von ausgewählten Aufgaben

Einstellung		Aktion
Status	**Ausführung erlauben**	Ausführung von ausgewählten Aufgaben nach dem festgelegten Zeitplan aktivieren, falls sie verboten wurden.
	Ausführung verbieten	Ausführung von ausgewählten Aufgaben verbieten. Aufgaben bleiben dabei in der Liste erhalten, werden aber nicht ausgeführt.

Einstellung		Aktion
		Die gleiche Aktion kann alternativ im Aufgabeneditor auf der Registerkarte **Allgemein** durch Aktivieren des Kontrollkästchens **Ausführung erlauben** durchgeführt werden.
Schweregrad	**Kritisch machen**	Die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Agents** erzwingen, falls die geplante Ausführung versäumt wurde.
	Nicht kritisch machen	Die Aufgabe nur zur festgelegten Zeit ausführen lassen, unabhängig davon, ob die Ausführung der Aufgabe übersprungen wurde.
		Die gleiche Aktion kann alternativ im Aufgabeneditor auf der Registerkarte **Allgemein** durch Aktivieren des Kontrollkästchens **Kritische Aufgabe** durchgeführt werden.
Einstellungen duplizieren		Die in der Liste des aktuellen Zeitplans gewählten Aufgaben duplizieren. Beim Aktivieren der Option **Einstellungen duplizieren** werden neue Aufgaben mit den Einstellungen erstellt, die den gewählten Aufgaben entsprechen.
Wiederholt planen		Diese Option gilt nur für einmalige Aufgaben: die Aufgabe noch einmal entsprechend den festgelegten Zeiteinstellungen ausführen lassen. Informationen zur Anzahl der Aufgabenausführung finden Sie im Unterabschnitt Aufgabeneditor.
Ausgewählte Aufgaben löschen		Ausgewählte Aufgabe aus dem Zeitplan entfernen.

3. Um die Parameter einer Aufgabe zu bearbeiten, wählen Sie diese in der Aufgabenliste. Das Fenster **Aufgaben-Editor** wird geöffnet. Seine Beschreibung finden Sie unten.
4. Sobald Sie mit der Bearbeitung des Zeitplans fertig sind, klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Aufgaben-Editor

Im Aufgabeneditor können Sie Einstellungen für die folgenden Zwecke festlegen:

1. Erstellung einer neuen Aufgabe.

   Klicken Sie dafür auf der Symbolleiste auf **Aufgabe erstellen**.

2. Bestehende Aufgabe bearbeiten.

   Klicken Sie dafür in der Aufgabenliste auf den Namen der gewünschten Aufgabe.

Das Fenster zur Bearbeitung der Aufgabenparameter wird angezeigt. Die Einstellungen bei der Bearbeitung einer bestehenden Aufgabe entsprechen denen bei der Erstellung einer neuen Aufgabe.

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

So bearbeiten Sie die Parameter einer Aufgabe

1. Auf der Registerkarte **Allgemein** werden die folgenden Parameter konfiguriert:
   - Im Feld **Name** wird der Name der Aufgabe festgelegt, unter dem sie im Zeitplan angezeigt wird.
   - Um die Aufgabe ausführen zu lassen, aktivieren Sie das Kontrollkästchen **Ausführung zulassen**. Beim deaktivierten Kontrollkästchen wird die Aufgabe in der Liste zwar angezeigt, doch nicht ausgeführt.

Alterativ können Sie dafür die Option **Status** verwenden, die sich im Hauptfenster des Editors auf der Symbolleiste befindet.

- Das aktivierte Kontrollkästchen **Kritische Aufgabe** erzwingt die Ausführung der Aufgabe beim nächsten Start des **Dr.Web Servers**, falls die geplante Ausführung versäumt wurde (**Dr.Web Server** ist zum Zeitpunkt der Aufgabenausführung deaktiviert). Wenn die Aufgabe innerhalb eines Zeitraums mehrmals nicht ausgeführt wurde, wird sie beim Start des **Dr.Web Servers** nur einmal ausgeführt.

Alternativ können Sie dafür die Option **Schweregrad** verwenden, die sich im Hauptfenster des Editors auf der Symbolleiste befindet.

2. Wählen Sie auf der Registerkarte **Aktion** in der Dropdown-Liste **Aktion** einen Aufgabentyp aus und legen Sie die erforderlichen Parameter fest.

Tabelle 7-4: Typen und Parameter der Aufgaben

Aufgabentyp	Parameter und ihre Beschreibung
Prozedur ausführen	Diese Aufgabe dient zur Ausführung von benutzerdefinierten Prozeduren (mehr dazu finden Sie unter Benutzerprozeduren). Folgende Parameter müssen festgelegt werden: • **Gruppe der Prozeduren** – Gruppe von benutzerdefinierten Prozeduren, für welche die Prozedur ausgeführt werden soll. • **Prozedur** – Name der auszuführenden benutzerdefinierten Prozedur aus der Gruppe, die im der Liste **Gruppe der Prozeduren** gewählte wurde. • Aktivieren Sie das Kontrollkästchen **Für alle Gruppen der Prozeduren durchführen**, damit die gewählte benutzerdefinierte Prozedur in allen Gruppen von Prozeduren ausgeführt wird, in denen sie festgelegt wurde. Für jede Gruppe wird dabei die Prozedur ausgeführt, die für diese Gruppe festgelegt wurde.
Skript ausführen	Diese Aufgabe dient zur Ausführung des LUA-Skripts, das im Feld **Skript** angegeben ist.
Dr.Web Server herunterfahren	Diese Aufgabe beendet den **Server**. Für den Start sind keine zusätzlichen Parameter erforderlich.
Verschlüsselungsschlüssel ersetzen	Diese Aufgabe dient zum regelmäßigen Ersetzen der Verschlüsselungsschlüssel, darunter: • privater Schlüssel `drwcsd.pri` auf dem **Server**, • öffentlicher Schlüssel `drwcsd.pub` auf Workstations. Da einige Workstations zum Zeitpunkt des Ersatzes ausgeschaltet sein können, verläuft der Vorgang in zwei Schritten. Für jeden Schritt muss eine separate Aufgabe geplant werden. Der zweite Schritt sollte in einiger Zeit nach der Ausführung des ersten Schrittes ausgeführt werden. In dieser Zeit stellen einige Workstations möglicherweise eine Verbindung mit dem **Server** her. bei der Erstellung der Aufgabe müssen Sie in der Dropdown-Liste den entsprechenden Schritt auswählen: • **Neuen Schlüssel hinzufügen**. Das ist der erste Schritt des Vorgangs, in dem ein neues nicht aktives Schlüsselpaar erzeugt wird. Workstations erhalten einen neuen öffentlichen Schlüssel, wenn sie eine Verbindung mit dem **Server** herstellen. • **Alten Schlüssel löschen und zum neuen Schlüssel wechseln**. Das ist der zweite Schritt, in dem Workstations über den Wechsel zu neuen Schlüsseln benachrichtigt werden. Aktuelle Schlüssel werden dann durch neue Schlüssel ersetzt, darunter öffentliche Schlüssel auf Workstations und privater Schlüssel auf dem **Server**.

Aufgabentyp	Parameter und ihre Beschreibung
	Die Workstations, die keinen neuen öffentlichen Schlüssel erhalten haben, können keine Verbindung mit dem **Server** herstellen. Um dieses Problem zu beheben, können Sie wie folgt vorgehen: • Kopieren Sie einen neuen öffentlichen Schlüssel auf die Workstations (lesen Sie im Dokument **Anhänge** unter Dr.Web Agent mit einem anderen Dr.Web Server verbinden, wie Sie den Schlüssel auf einer Workstation ersetzen können). • Erlauben Sie den **Agents** die Autorisierung auf dem **Server** mit dem ungültigen öffentlichen Schlüssel (s. dazu den Bereich Netzwerk in den Einstellungen des **Agents**).
In die Protokolldatei eintragen	Diese Aufgabe lässt die festgelegte Zeile in die Protokolldatei des **Servers** schreiben. **Zeile** – Text der Meldung, die in die Protokolldatei geschrieben werden soll.
Programm starten	Die Aufgabe dient zum Start eines beliebigen Programms. Folgende Parameter müssen festgelegt werden: • Geben Sie im Feld **Pfad** den vollständigen Namen (mit der Pfadangabe) der ausführbaren Datei des Programms an, das gestartet werden soll. • Geben Sie im Feld **Argumente** Befehlszeilenparameter für das auszuführende Programm an. • Aktivieren Sie das Kontrollkästchen **Synchron ausführen**, um die Synchronisierung mit dem **Server** zu ermöglichen: Das Programm wird beendet, bevor die Ausführung anderer Aufgaben des Typs **Programm starten** beginnt. Wenn das Kontrollkästchen **Synchron ausführen** deaktiviert ist, protokolliert der **Server** nur den Start des Programms. Wenn das Kontrollkästchen **Synchron ausführen** aktiviert ist, protokolliert der **Server** den Start des Programms, seinen Rückgabecode und seine Endzeit.
Erinnerung an den Lizenzablauf	Diese Aufgabe dient zur Benachrichtigung über den Lizenzablauf für das **Dr.Web** Produkt. Sie müssen den Zeitraum bis zum Ablauf der Lizenz angeben, ab dem die entsprechende Benachrichtigung angezeigt werden soll.
Repository aktualisieren	Mehr zur Aufgabe finden Sie unter Geplante Aktualisierungen.
Meldung an Workstation senden	Mit dieser Aufgaben senden Sie an Benutzer einer Workstations oder Gruppe von Workstations eine Meldung. Die Einstellungen sind im Abschnitt Nachrichten an Workstations unter Windows® versenden zu finden.
Datenbank bereinigen	Die Aufgabe dient zum Sammeln und Löschen nicht verwendeter Einträge in der Datenbank des **Servers**. Die Aufgabe wird mithilfe des Befehls `vacuum` ausgeführt. Für den Start sind keine zusätzlichen Parameter erforderlich.
Nicht abgesendete Ereignisse bereinigen	Diese Aufgabe dient zum Löschen nicht gesendeter Ereignisse in der Datenbank. Geben Sie den Zeitraum für die Speicherung nicht gesendeter Ereignisse, nach dessen Ablauf solche Ereignisse gelöscht werden sollen. Es handelt sich um Ereignisse, die von einem untergeordneten **Server** an den übergeordneten **Server** gesendet werden. Wenn der Sendeversuch fehlgeschlagen ist, wird das Ereignis in die Liste nicht gesendeter Ereignisse verschoben. Der untergeordnete **Server** sendet Ereignisse im festgelegten Zeitintervall. Nachdem die Aufgabe **Nicht abgesendete Ereignisse bereinigen** ausgeführt wurde, werden alle Ereignisse, die länger als angegeben aufbewahrt werden, gelöscht.
Alte Einträge bereinigen	Diese Aufgabe dient zum Löschen nicht aktueller Informationen in der Datenbank. Geben Sie die Anzahl von Tagen an, nach denen statistische Daten über Workstations (nicht die Workstations selbst) als alt eingestuft werden und auf dem **Server** gelöscht werden sollen.

Aufgabentyp	Parameter und ihre Beschreibung
	Der Zeitraum, nach dessen Ablauf statistische Daten gelöscht werden, wird für jeden Typ der Einträge individuell festgelegt.
Alte Stationen bereinigen	Diese Aufgabe dient zum Löschen nicht aktueller Workstations in der Datenbank. Geben Sie den Zeitraum (der Standardwert beträgt 90 Tage) an, in dem die Workstations, die keine Verbindung mit dem **Server** hergestellt haben, als nicht aktuell eingestuft werden und auf dem **Server** gelöscht werden sollen.
Dr.Web Server neu starten	Diese Aufgabe dient zum Neustart des **Servers**. Für den Start sind keine zusätzlichen Parameter erforderlich.
Aufwecken von Stationen	Diese Aufgabe dient zur Aktivierung von Workstations, beispielsweise vor der Ausführung einer Scan-Aufgabe. Die unterstehenden Einstellungen bestimmen, welche Workstations aktiviert werden sollen. • **Alle Stationen wecken**. Diese Option gibt an, dass alle mit dem **Server** verbundenen Workstations aktiviert werden sollen. • **Stationen nach festgelegten Parametern wecken**. Diese Option gibt an, dass nur die Workstations, die den unterstehenden Parametern entsprechen, aktiviert werden sollen: ○ **IP-Adressen**. Hier werden IP-Adressen der Workstations aufgelistet, die aktiviert werden sollen. Adressen müssen im Format 10.3.0.127, 10.4.0.1-10.4.0.5 oder 10.5.0.1/30 angegeben werden. Um mehre Adressen anzugeben, verwenden Sie ein Komma oder einen Zeilenumbruch. IP-Adressen können durch DNS-Namen ersetzt werden. ○ **MAC-Adressen**. Hier werden MAC-Adressen der Workstations aufgelistet, die aktiviert werden sollen. Die Oktetts einer MAC-Adresse müssen durch das Zeichen „:" getrennt werden. Um mehrere Adressen anzugeben, verwenden Sie ein Komma oder einen Zeilenumbruch. ○ **Gruppenidentifikatoren**. Hier werden IDs der Gruppen aufgelistet, deren Workstations aktiviert werden sollen. Verwenden Sie für jede neue ID ein einzelnes Feld. Um ein neues Feld hinzuzufügen, klicken Sie auf . Um ein Feld zu entfernen, klicken Sie neben der zu entfernenden ID auf . Für die Ausführung dieser Aufgabe müssen auf den zu aktivierenden Workstations WOL-taugliche Netzwerkkarten installiert werden. Ob Ihre Netzwerkkarte die Funktion Wake-on-LAN unterstützt, entnehmen Sie der Dokumentation oder den Eigenschaften der Netzwerkkarte (**Control Panel → Network and Internet → Network Connections → Change Adapter Settings → Configure → Advanced**).
Sicherung kritischer Daten des Servers	Die Aufgabe dient zur Sicherung von kritischen Daten des **Servers**, darunter: • Datenbank • Lizenzschlüsseldatei • Privater Schlüssel Folgende Parameter müssen festgelegt werden: • **Pfad –** Pfad des Verzeichnisses, in dem die Daten gespeichert werden sollen (wenn das Feld leer ist, wird das Standardverzeichnis verwendet). • **Maximale Anzahl der Kopien –** maximale Anzahl von Sicherungskopien. Ein Nullwert gibt an, dass es keine Einschränkung gibt. Weitere Informationen finden Sie im Dokument **Anhänge** unter Anhang H3.5.
Repository sichern	Diese Aufgabe dient zur regelmäßigen Sicherung des Repository.

Aufgabentyp	Parameter und ihre Beschreibung

	Folgende Parameter müssen festgelegt werden:
	• **Pfad** – der vollständige Pfad des Verzeichnisses, in dem Sicherungskopien abgespeichert werden sollen.
	• **Maximale Anzahl der Kopien** – maximale Anzahl von Sicherungskopien des Repository, die im angegebenen Verzeichnis gespeichert werden. Wenn die maximal zulässige Anzahl an Repository-Kopien erreicht wird, wird die älteste der vorhandenen Kopien gelöscht, damit eine neue Sicherungskopie gespeichert wird.
	• **Repository-Bereich**. Diese Option gibt an, welche Informationen zur Antivirenkomponente gespeichert werden sollen. Drei Varianten sind möglich:
	  ○ **Das ganze Repository** – alle Repository-Revisionen der in der Liste unten gewählten Komponenten werden gespeichert.
	  ○ **Nur kritische Revisionen** – nur die als kritisch markierten Revisionen der in der Liste unten gewählten Komponenten werden gespeichert.
	  ○ **Nur Konfigurationsdateien** – nur Konfigurationsdateien der in der Liste unten gewählten Komponenten werden gespeichert.
	• Aktivieren Sie das Kontrollkästchen neben den Komponenten, deren gewählte Bereiche gespeichert werden sollen.

Mit Active Directory synchronisieren	Diese Aufgabe wird zur Synchronisierung des Netzwerks verwendet: Active Directory-Container, die Rechner enthalten, werden zu Gruppen des Antivirus-Netzwerks, in die Workstations verschoben werden. Für den Start sind keine zusätzlichen Parameter erforderlich. Diese Aufgabe ist standardmäßig deaktiviert. Um die Aufgabe zu aktivieren, aktivieren Sie in den Einstellungen der Aufgabe oder auf der Symbolleiste die Option **Ausführung erlauben**.
Es wurde seit langem keine Verbindung mit dem benachbarten Server hergestellt	Diese Aufgabe benachrichtigt, dass benachbarte **Server** seit langem keine Verbindung mit dem **Server** hergestellt haben. Die Anzeige der Benachrichtigung wird im Bereich Benachrichtigungskonfiguration über den Punkt **Es wurde seit langem keine Verbindung mit dem benachbarten Server hergestellt** eingestellt. Geben Sie in den Feldern **Stunden** und **Minuten** den Zeitraum an, nach dessen Ablauf ein benachbarter **Server** als seit langem nicht verbunden eingestuft werden soll.
Seit langem keine Verbindung zwischen der Station und dem Server	Diese Aufgabe benachrichtigt, dass Workstations seit langem keine Verbindung mit dem **Server** hergestellt haben. Die Anzeige der Benachrichtigung wird im Bereich Benachrichtigungskonfiguration über den Punkt **Seit langem keine Verbindung zwischen der Station und dem Server hergestellt** eingestellt. Geben Sie im Feld **Tage** den Zeitraum an, nach dessen Ablauf eine Workstation als seit langem nicht verbunden eingestuft werden soll.
Statistikberichte	Diese Aufgabe dient zum Erstellen von Berichten mit statistischen Daten zum Antivirus-Netzwerk. Damit der Bericht erstellt werden kann, muss die Benachrichtigung **Regelmäßiger Bericht** aktiviert werden (mehr dazu finden Sie unter Benachrichtigungskonfiguration). Der erstellte Bericht wird auf dem Rechner, auf dem der **Server** installiert ist, abgespeichert. Die Berichtsübermittlung ist auf den Benachrichtigungstyp angewiesen: • Bei der Sendemethode **E-Mail** wird an die in den Benachrichtigungseinstellungen festgelegte E-Mail-Adresse eine E-Mail gesendet, die neben einem Link zum Bericht auch den Bericht selbst angehängt enthält. • Bei allen anderen Sendemethoden wird eine Benachrichtigung gesendet, die den Link zum Bericht enthält.

Aufgabentyp	Parameter und ihre Beschreibung
	Um eine neue Aufgabe im Zeitplan zu erstellen, müssen Sie die folgenden Einstellungen festlegen: • **Benachrichtigungsprofile** – Name einer Gruppe von Benachrichtigungen mit den Einstellungen, anhand denen der entsprechende Bericht erstellt werden soll. Der Titelname wird beim Erstellen einer neuen Gruppe von Benachrichtigungen festgelegt. • **Berichtssprache** – Sprache, in der Daten im Bericht angezeigt werden sollen. • **Datumsformat** – Format, in dem Datumsangaben im Bericht angezeigt werden sollen. Möglich sind die folgenden Formate: o `DD-MM-YYYY HH:MM:SS` o `MM/DD/YYYY HH:MM:SS` • **Berichtsformat** – Format des Dokuments, in dem statistische Daten gespeichert werden sollen. • **Berichtsperiode** – Zeitraum, für den statistische Daten in den Bericht aufgenommen werden sollen. • **Gruppen** – Liste der Gruppen von Workstations im Antivirus-Netzwerk, für die Daten in den Bericht aufgenommen werden sollen. Um mehrere Gruppen auszuwählen, verwenden Sie die STRG- oder UMSCHALTTASTE. • **Berichtstabellen** – Liste der Tabellen mit Statistik, deren Daten in den Bericht aufgenommen werden sollen. Um mehrere Tabellen auszuwählen, verwenden Sie die STRG- oder UMSCHALTTASTE. • **Speicherfrist des Berichts** – Zeitraum, in dem Berichte auf dem Rechner, auf dem der **Server** installiert ist, gespeichert werden sollen. Der Aufbewahrungszeitraum beginnt mit dem Datum der Berichtserstellung.
Alte Nachrichten löschen	Diese Aufgabe dient zum Löschen der folgenden in der Datenbank enthaltenen Nachrichten: • Benachrichtigungen des Agents • Benachrichtigungen für die Web-Konsole • Nach Zeitplan erstellte Protokolle Gelöscht werden die als veraltet markierten Nachrichten. Es handelt sich dabei um Nachrichten mit abgelaufener Aufbewahrungsfrist. Diese Frist kann wie folgt festgelegt werden. • Für Benachrichtigungen: bei der Erstellung von Benachrichtigungen für die jeweilige Sendemethode (mehr dazu finden Sie unter Benachrichtigungskonfiguration). • Für Protokolle: in der Aufgabe zur Erstellung von Protokollen. Für den Start der Aufgabe sind keine zusätzlichen Parameter erforderlich.

Um Speicherplatz zu sparen, werden veraltete Informationen in der Datenbank gelöscht. Der Standardwert für die Aufgaben **Alte Stationen bereinigen** und **Alte Einträge bereinigen** beträgt 90 Tage. Wenn Sie diesen Wert verringern, wird die erfasste Statistik zu Komponenten des Antivirus-Netzwerks weniger repräsentativ. Ein größerer Wert kann hingegen die Leistung des **Servers** stark beeinträchtigen.

Wenn die Aufgabe **Skript ausführen** auf mehreren **Servern**, welche die gleiche Datenbank verwenden, gleichzeitig ausgeführt wird, können Fehler bei der Ausführung dieser Aufgabe auftreten.

3. Auf der Registerkarte **Zeit**:
   - Wählen Sie in der Dropdown-Liste **Periode** einen Startmodus für die Aufgabe und geben Sie an, wie häufig die Aufgabe wiederholt werden soll.

Tabelle 7-5: Startmodi und ihre Parameter

Startmodus	Parameter und ihre Beschreibung
Abschließend	Die Aufgabe wird ausgeführt, sobald der **Server** heruntergefahren ist. Für den Start sind keine zusätzlichen Parameter erforderlich.
Anfänglich	Die Aufgabe wird nach dem Start des **Servers** ausgeführt. Für den Start sind keine zusätzlichen Parameter erforderlich.
In N Minuten nach Anfangsaufgabe	Wählen Sie in der Dropdown-Liste **Anfangsaufgabe** die Aufgabe, die als Referenz für die Ausführungszeit der aktuellen Aufgabe dienen soll. Geben Sie im Feld **Minute** die Zeit in Minuten an bzw. wählen Sie diese in der Liste aus, die nach der Ausführung der Anfangsaufgabe vergehen muss, damit die Ausführung der zu bearbeitenden Aufgabe beginnt.
Täglich	Geben Sie die Uhrzeit an, zu der die Aufgabe täglich ausgeführt werden soll.
Monatlich	Geben Sie das Datum und die Uhrzeit an, an dem die Aufgabe monatlich ausgeführt werden soll.
Wöchentlich	Geben Sie den Tag und die Uhrzeit an, an dem die Aufgabe wöchentlich ausgeführt werden soll.
Stündlich	Geben Sie eine Zahl von 0 bis 59 ein: Die Aufgabe wird stündlich zur eingegebenen Minute gestartet.
Alle N Minuten	Geben Sie den Wert **N** ein, um ein Intervall zwischen Aufgaben festzulegen. Wenn der Wert **N** 60 oder mehr beträgt, wird die Aufgabe alle **N** Minuten ausgeführt. Wenn der Wert **N** weniger als 60 beträgt, wird die Aufgabe zu jeder Minute der Stunde, die durch **N** teilbar ist, gestartet.

   - Aktivieren Sie das Kontrollkästchen **Nach der ersten Ausführung verbieten**, damit die Aufgabe zum festgelegten Zeitpunkt einmalig ausgeführt wird. Wenn das Kontrollkästchen deaktiviert ist, wird die Aufgabe mit der angegebenen Häufigkeit mehrmals ausgeführt.

   Damit die bereits ausgeführte einmalige Aufgabe erneut ausgeführt wird, klicken Sie auf der Symbolleiste des Zeitplan-Bereichs auf **Wiederholt planen**.

4. Sobald Sie mit der Bearbeitung der Aufgabenparameter fertig sind, klicken Sie auf **Speichern**, um die vorgenommenen Änderungen zu übernehmen (falls Sie eine bereits bestehende Aufgabe bearbeitet haben) bzw. um eine neue Aufgabe mit den festgelegten Parametern zu erstellen (falls Sie eine neue Aufgabe erstellt haben).

7.5. Webserver konfigurieren

So konfigurieren Sie den Webserver

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster den Punkt des Verwaltungsmenüs **Konfiguration des Webservers**. Das Fenster zum Einstellen des **Webservers** wird angezeigt.

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

3. Auf der Symbolleiste sind die folgenden Schaltflächen verfügbar:

   Dr.Web Server neu starten. Mit dieser Option können Sie den **Server** neu starten, damit die im Bereich vorgenommenen Änderungen wirksam werden. Diese Schaltfläche wird anklickbar, sobald Änderungen an den Einstellungen vorgenommen wurden und die Schaltfläche **Speichern** angeklickt wurde.

   Konfiguration aus Backup wiederherstellen. Bei dieser Option handelt es sich um eine Dropdown-Liste, die gespeicherte Kopien der Einstellungen des Bereichs enthält. Diese Einstellungen können bei Bedarf wiederhergestellt werden. Diese Schaltfläche wird anklickbar, sobald Änderungen an den Einstellungen vorgenommen wurden und die Schaltfläche **Speichern** angeklickt wurde.

   Alle Parameter mit den ursprünglichen Werten wiederherstellen. Diese Option gibt an, dass die ursprünglichen (zuletzt gespeicherten) Werte aller Einstellungen des Bereichs wiederhergestellt werden sollen.

   Defaultparameter wiederherstellen. Diese Option gibt an, dass die Standardwerte aller Einstellungen des Bereichs wiederhergestellt werden sollen.
4. Damit die Änderungen an den Einstellungen des Bereichs wirksam werden, klicken Sie auf **Speichern** und starten Sie den **Server** neu. Klicken Sie dafür auf der Symbolleiste des Bereichs auf **Dr.Web Server neu starten**.

7.5.1. Allgemein

Auf der Registerkarte **Allgemein** können Sie die folgenden Einstellungen des **Webservers** konfigurieren:

- **Server** – Name des **Dr.Web Servers**.

  Der Wert dieser Option muss im folgenden Format angegeben werden:

  <IP-Adresse oder DNS-Name des Servers>`[:`*<Port>*`]`

  Wenn keine Adresse des **Servers** angegeben ist, wird der vom Betriebssystem zurückgegebene Name des Rechners oder Netzwerkadresse des **Servers** verwendet: DNS-Name, falls vorhanden, anderenfalls IP-Adresse.

  Wenn keine Portnummer angegeben ist, wird der Port verwendet, der in der Anforderung angegeben wurde (beispielsweise, wenn auf den **Server** über das **Verwaltungscenter** oder **Web API** zugegriffen wird) . Bei Anforderungen über das **Verwaltungscenter** ist das der Port, der in der Adresszeile bei der Verbindung des **Verwaltungscenters** mit dem **Server** angegeben wurde.

  Der Wert wird im Parameter `<server-name />` der Konfigurationsdatei `webmin.conf` gespeichert.

  Der Wert dieser Einstellung wird auch beim Generieren des Links zum Herunterladen der Installationsdatei des **Agents** für Workstations des Antivirus-Netzwerks verwendet.
- **Parallele Anfragen** – Anzahl gleichzeitiger Abfragen, die vom **Webserver** verarbeitet werden. Diese Option beeinflusst die Leistung des **Servers**. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.
- **IO Threads** – Anzahl von Threads, welche die über das Netzwerk übertragenen Daten verarbeiten. Diese Option beeinflusst die Leistung des **Servers**. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.
- **Timeout (Sek.)** – HTTP-Sitzungszeitlimit. Bei ständigen Verbindungen wird die Verbindung mit dem **Server** getrennt, wenn keine Anforderungen des Clients innerhalb des angegebenen Zeitraums empfangen wurden.
- **Minimale Senderate (Bit/s)** – minimal zulässige Senderate. Wenn die Übertragungsgeschwindigkeit der ausgehenden Netzwerkverbindungen diesen Wert unterschreitet, wird keine Verbindung hergestellt. Geben Sie 0 an, um diese Einschränkung aufzuheben.

- **Minimale Empfangsrate (B/s)** – minimal zulässige Empfangsrate. Wenn die Übertragungsgeschwindigkeit der eingehenden Netzwerkverbindungen diesen Wert unterschreitet, wird keine Verbindung hergestellt. Geben Sie 0 an, um diese Einschränkung aufzuheben.
- **Größe des Sendepuffers (KB)** – Größe des Sendepuffers. Diese Option beeinflusst die Leistung des **Servers**. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.
- **Größe des Empfangspuffers (KB)** – Größe des Empfangspuffers. Diese Option beeinflusst die Leistung des **Servers**. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.
- **Maximale Anforderungslänge (KB)** – maximal zulässige Länge einer HTTP-Anforderung.
- **Komprimierung verwenden**. Aktivieren Sie das Kontrollkästchen, um Datenverkehr bei der HTTP/HTTPS-Kommunikation mit dem **Webserver** zu komprimieren.
  - Wenn Sie das Kontrollkästchen aktiviert ist, wird die Dropdown-Liste **Komprimierungsstufe** verfügbar. In dieser Liste können Sie eine Zahl im Bereich von 0 bis 9 auswählen, wobei die Eins die minimale und die Neun die maximale Komprimierungsstufe ist.
- **IP-Adressen ersetzen**. Aktivieren Sie das Kontrollkästchen, um in der Protokolldatei des **Servers** IP-Adressen durch DNS-Namen der Rechner zu ersetzen.
- **SSL-Sitzung aktiv halten**. Aktivieren Sie das Kontrollkästchen, um die Keep-Alive-Verbindung für SSL-gesicherte Verbindungen zu verwenden. Beachten Sie, dass einige alte Browser-Versionen reguläre SSL-Verbindungen nicht unterstützen. Deaktivieren Sie diese Option, falls Sie Probleme mit dem SSL-Verbindungsaufbau vermuten.
- **SSL-Zertifikat**. Hier wird der Pfad zum SSL-Zertifikat angegeben. Die Dropdown-Liste enthält alle im Verzeichnis des **Servers** verfügbaren Zertifikate.
- **Privater SSL-Schlüssel**. Hier wird der Pfad zum privaten SSL-Schlüssel angegeben. Die Dropdown-Liste enthält alle im Verzeichnis des **Servers** verfügbaren privaten SSL-Schlüssel.

7.5.2. Optionen

Auf der Registerkarte **Optionen** können Sie die Einstellungen für den **Webserver** konfigurieren:

- Aktivieren Sie das Kontrollkästchen **Scriptfehler anzeigen**, um Scriptfehler im Webbrowser anzuzeigen. Diese Option wird vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.
- Aktivieren Sie das Kontrollkästchen **Script-Ausführungen verfolgen**, um Informationen über die Ablaufverfolgung beim Ausführen der Scripts des Servers zu protokollieren. Diese Option wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.
- Aktivieren Sie das Kontrollkästchen **Script-Ausführungen abbrechen**, um den Abbruch eines Scripts während der Ausführung zuzulassen. Diese Option wird hauptsächlich vom technischen Support und Software-Entwicklern verwendet. Ändern Sie den vorgegebenen Wert nur bei dringendem Bedarf.

7.5.3. Transport

Auf der Registerkarte **Transport** werden Netzwerkadressen angegeben, an denen der **Webserver** lauscht, um eingehende Verbindungen anzunehmen. Diese werden zur Verbindung mit dem **Verwaltungscenter** oder zur Ausführung von Anforderungen über Web API verwendet:

- In Bereich **Adressen, die mit HTTP abgehört werden** werden Schnittstellen angegeben, an denen zur Annahme von HTTP-Verbindungen gelauscht werden soll:

  Geben Sie in den Feldern **Adresse** und **Port** die IP-Adresse und Portnummer der Netzwerkschnittstelle an, von der aus HTTP-Verbindungen angenommen werden können.

Standardmäßig lauscht der **Webserver** an den folgenden Netzwerkschnittstellen und Ports:

- **Adresse**: `0.0.0.0` – „alle Netzwerkschnittstellen" für den Rechner verwenden, auf dem der **Webserver** installiert ist.
- **Port**: `9080` – Standardport `9080` für das HTTP-Protokoll verwenden.

◆ In Bereich **Adressen, die mit HTTPS abgehört werden** werden Schnittstellen angegeben, an die zur Annahme von HTTPS-Verbindungen gelauscht werden soll:

Geben Sie in den Feldern **Adresse** und **Port** die IP-Adresse und Portnummer der Netzwerkschnittstelle an, von der aus HTTPS-Verbindungen angenommen werden können.

Standardmäßig lauscht der **Webserver** an den folgenden Netzwerkschnittstellen und Ports:

- **Adresse**: `0.0.0.0` – „alle Netzwerkschnittstellen" für den Rechner verwenden, auf dem der **Webserver** installiert ist.
- **Port**: `9081` – Standardport `9081` für das HTTPS-Protokoll verwenden.

Um ein neues Feld hinzuzufügen, klicken Sie im entsprechenden Bereich auf die Schaltfläche . Um ein vorhandenes Feld zu entfernen, klicken neben dem zu entfernenden Feld auf .

7.5.4. Sicherheit

Auf der Registerkarte **Sicherheit** können Sie Einschränkungen für die Netzwerkadressen festlegen, von denen aus der **Webserver** HTTP- und HTTPS-Anforderungen empfangen soll.

So legen Sie Zugriffseinschränkungen für einen Verbindungstyp fest

1. Um den HTTP- bzw. HTTPS-Zugriff von bestimmten Adressen zuzulassen, fügen Sie diese Adressen zur Liste **HTTP: erlaubt** bzw. **HTTPS: erlaubt** hinzu.
2. Um den HTTP- bzw. HTTPS-Zugriff von bestimmten Adressen zu verbieten, fügen Sie diese Adressen zur Liste **HTTP: verboten** bzw. **HTTPS: verboten** hinzu.
3. Adressen, die keiner der Listen hinzugefügt wurden, werden je nach dem, ob das Kontrollkästchen **Priorität des Verbots für HTTP** und **Priorität des Verbots für HTTPS** aktiviert ist: Wenn das Kontrollkästchen aktiviert ist, werden die Adressen, die keiner Liste bzw. beiden Listen hinzugefügt sind, nicht zugelassen. Anderenfalls sind diese Adressen erlaubt.

So bearbeiten Sie die Liste von Adressen

1. Geben Sie ins entsprechende Feld die gewünschte Netzwerkadresse ein und klicken Sie dann auf **Speichern**.
2. Die Netzwerkadresse muss wie folgt angegeben werden: *<IP-Adresse>*`/[`*<Präfix>*`]`.

Listen für TCPv6-Adressen werden nur dann eingeblendet, wenn der Rechner über die IPv6-Schnittstelle verfügt.

3. Um ein neues Feld hinzuzufügen, klicken Sie im entsprechenden Bereich auf die Schaltfläche .
4. Um ein Feld zu löschen, klicken Sie auf .

Beispiel für einen Präfix:

1. Das Präfix 24 steht für Netzwerke mit einer Subnetzmaske: `255.255.255.0`

   Beinhaltet 254 Adressen

   Hostadressen in diesen Netzwerken sehen so aus: `195.136.12.*`

2. Das Präfix 8 steht für Netzwerke mit einer Subnetzmaske: `255.0.0.0`

Beinhaltet bis zu 16387064 Adressen (256*256*256)

Hostadressen in diesen Netzwerken sehen so aus: `125.*.*.*`

7.6. Benutzerprozeduren

Um die Ausführung häufiger Aufgaben des **Dr.Web Servers** zu vereinfachen und automatisieren, können verschiedene benutzerdefinierte Prozeduren verwendet werden. Diese Prozeduren basieren auf Lua-Scripts.

Benutzerdefinierte Prozeduren befinden sich im folgenden Unterverzeichnis vom Installationsverzeichnis des **Servers**:

- Unter Windows: `var\extensions`
- Unter FreeBSD: `/var/drwcs/extensions`
- Unter Linux und Solaris: `/var/opt/drwcs/extensions`

Nach der Installation des **Servers** befinden sich in diesem Unterverzeichnis vorinstallierte benutzerdefinierte Prozeduren.

Benutzerdefinierte Prozeduren sollten über das **Verwaltungscenter** bearbeitet werden.

So passen Sie benutzerdefinierte Prozeduren an

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster den Punkt des Verwaltungsmenüs **Benutzerprozeduren**. Das Fenster für die Konfiguration benutzerdefinierter Prozeduren wird geöffnet.

Baumstruktur von Prozeduren

Prozeduren werden in der Baumansicht angezeigt. Gruppen von Prozeduren und dazu gehörende benutzerdefinierte Prozeduren stellen die Knoten dieser Baumstruktur dar.

Standardmäßig beinhaltet die Baumstruktur der Prozeduren die vorinstallierte Gruppe **Examples of the hooks**, die Vorlagen für alle verfügbaren benutzerdefinierten Prozeduren enthält. Anhand dieser Vorlagen können Sie Ihre eigenen benutzerdefinierten Prozeduren erstellen.

Prozeduren verwalten

Zur Verwaltung von Prozeduren sind auf der Symbolleiste die folgenden Elemente verfügbar:

– Dropdown-Liste, in der Sie ein Element zur Baumstruktur der Prozeduren hinzufügen können. Verwenden Sie dafür die folgenden Schaltflächen:

Prozedur hinzufügen – eine neue auf der Vorlage basierende benutzerdefinierte Prozedur hinzufügen.

Gruppe der Prozeduren hinzufügen – eine neue benutzerdefinierte Gruppe für Prozeduren erstellen.

Ausgewählte Objekte entfernen – eine in der Baumstruktur von Prozeduren gewählte benutzerdefinierte Prozedur bzw. Gruppe der Prozeduren entfernen.

Ausführen der Prozedur erlauben – die gleiche Aktion kann im Prozedureneditor durch Aktivierung des Kontrollkästchens **Ausführen der Prozedur erlauben** durchgeführt werden.

Ausführen der Prozedur verbieten – die gleiche Aktion kann im Prozedureneditor durch Aktivierung des Kontrollkästchens **Ausführen der Prozedur verbieten** durchgeführt werden.

7.7. Benachrichtigungen konfigurieren

Dr.Web Enterprise Security Suite kann Benachrichtigungen über Virusangriffe, Status der Antivirenkomponenten und sonstige Ereignisse an Administratoren des Antivirus-Netzwerks von **Dr.Web Enterprise Security Suite** versenden.

7.7.1. Benachrichtigungskonfiguration

So konfigurieren Sie Benachrichtigungen über Ereignisse im Antivirus-Netzwerk

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Konfiguration von Benachrichtigungen**.
2. Standardmäßig enthält die Liste keine Benachrichtigungen. Klicken Sie auf **Benachrichtigung hinzufügen**.
3. Um Benachrichtigungen versenden zu können, bringen Sie den Schalter links vom Namen des Benachrichtigungsprofils in die gewünschte Position:

   – Versand der Benachrichtigungen dieses Profils aktiviert.

   – Versand der Benachrichtigungen dieses Profils deaktiviert.
4. In diesem Bereich können Sie mehrere Benachrichtigungsprofile, z. B. für verschiedene Sendemethoden, erstellen. Um ein weiteres Profil hinzuzufügen, klicken Sie auf rechts von den Einstellungen des Benachrichtigungsprofils. Im unteren Teil der Seite wird ein neues Profil angezeigt. Einzelne Profile sowie Texte ihrer Vorlagen werden unabhängig voneinander konfiguriert.
5. Geben Sie im Feld **Überschrift** den Namen des zu erstellenden Profils. Dieser Name wird bei der Konfiguration der Aufgabe **Statistikberichte** im Zeitplan des **Servers** verwendet. Um den Namen nachträglich zu ändern, klicken Sie mit der linken Maustaste auf den Titel und geben Sie den gewünschten Namen ein. Wenn mehrere Profile vorhanden sind, wird beim Anklicken der Überschrift eine Dropdown-Liste angezeigt, in der alle vorhandenen Profile aufgelistet werden.
6. Um den Versand von Benachrichtigungen zu konfigurieren, wählen Sie in der Dropdown-Liste **Versandart von Benachrichtigungen** die gewünschte Sendemethode:
   - Web-Konsole – Benachrichtigungen werden in der Web-Konsole angezeigt.
   - Dr.Web Agent – Benachrichtigungen werden über das Protokoll des **Agents** versendet.
   - E-Mail – Benachrichtigungen werden per E-Mail versendet.
   - SNMP – Benachrichtigungen werden über das SNMP-Protokoll versendet.
   - Push-Benachrichtigungen – Versand von Push-Benachrichtigungen an das **Dr.Web Mobile Sicherheitscenter**. Dieser Punkt ist in der Dropdown-Liste **Versandart der E-Mail** nur dann verfügbar, falls das **Dr.Web Mobile Sicherheitscenter** mit dem **Dr.Web Server** verbunden ist.
   - Windows Message– Benachrichtigungen werden über den **Windows Nachrichtendienst** versendet (nur für **Server** unter Windows).

   Die einzelnen Einstellungen werden nachfolgend beschrieben.
7. Ihnen steht eine Reihe von Standardbenachrichtigungen des **Servers** zur Verfügung.

Die Beschreibung vordefinierter Benachrichtigungen und deren Parameter können Sie im Dokument **Anhänge** unter Anhang D1. Vordefinierte Benachrichtigungen finden.

So konfigurieren Sie Ihre individuellen Benachrichtigungen

a) Aktivieren Sie in der Liste von Benachrichtigungen die Kontrollkästchen neben den Benachrichtigungen, die entsprechend der für das Profil festgelegten Sendemethode versendet werden sollen.

b) Um die Einstellungen für Benachrichtigungen zu ändern, klicken Sie auf ⚙ neben der zu bearbeitenden Benachrichtigung. Eine Benachrichtigungsvorlage wird angezeigt. Bearbeiten Sie bei Bedarf den Text der Benachrichtigung. Im Text einer Benachrichtigung können Variablen (in Klammern) verwendet werden. Um eine Variable hinzuzufügen, verwenden Sie die Dropdown-Listen auf der oberen Leiste der Benachrichtigung. Beim Generieren der Benachrichtigung werden Vorlagenvariablen durch einen einstellungsabhängigen Text ersetzt. Verfügbare Variablen sind im Dokument **Anhänge** im Anhang D3. Parameter für Vorlagen des Benachrichtigungssystems aufgelistet.

c) Für Benachrichtigungen im Bereich **Workstation** können Sie Workstations angeben, die überwacht werden sollen. Wählen Sie in der Baumstruktur **Gruppen der überwachten Workstations** im Fenster zum Bearbeiten von Vorlagen einige Gruppen der Workstations, die überwacht werden sollen. Falls ein Ereignis auf einer dieser Workstations registriert wurde, wird eine entsprechende Benachrichtigung gesendet. Zur Mehrfachauswahl verwenden Sie die STRG oder UMSCHALTTASTE.

Beim Versand von Benachrichtigungen über das **SNMP**-Protokoll müssen ihre Texte im SNMP-Client angegeben werden. Über das **Verwaltungscenter** im Unterbereich **Workstation** können Sie nur Workstations angeben, die überwacht werden.

8. Wenn Sie mit der Bearbeitung fertig sind, klicken Sie auf **Speichern**, damit die vorgenommenen Änderungen wirksam werden.

Benachrichtigungen in der Web-Konsole

Um Benachrichtigungen in der **Web-Konsole** anzeigen zu lassen, legen Sie die folgenden Einstellungen fest:

- **Anzahl der erneuten Sendevorgänge**. Hier wird die Anzahl der Wiederholungsversuche nach einem Fehler beim Senden der Benachrichtigung angegeben. Der Standardwert beträgt 10.
- **Time-out des wiederholten Sendeversuchs**. Hier wird die Zeitspanne in Sekunden angegeben, die gewartet werden soll, bevor eine Benachrichtigung erneut versendet wird. Der Standardwert beträgt 300 Sekunden.
- **Speicherzeit der E-Mail**. Hier wird der Zeitraum angegeben, in dem eine erhaltene Benachrichtigung aufbewahrt werden soll. Der Standardwert beträgt 1 Tag. Wenn der angegebene Aufbewahrungszeitraum überschritten ist, wird die Benachrichtigung als veraltet gekennzeichnet und entsprechend der Aufgabe **Alte Nachrichten löschen** in den Einstellungen des **Servers** gelöscht.

  Für diese Benachrichtigungen können Sie im Bereich Benachrichtigungen der Web-Konsole einen zeitlich unbegrenzten Aufbewahrungszeitraum festlegen.

- **Testnachricht senden**. Diese Option gibt an, dass eine Testbenachrichtigung entsprechend den festgelegten Einstellungen des Benachrichtigungssystems gesendet werden soll. Der Text einer Testbenachrichtigung kann in der jeweiligen Vorlage angegeben werden.

Benachrichtigungen über das Protokoll des Agents

Um Benachrichtigungen über das Protokoll des **Agents** versenden zu können, legen Sie die folgenden Einstellungen fest:

- **Anzahl der erneuten Sendevorgänge**. Hier wird die Anzahl der Wiederholungsversuche nach einem Fehler beim Senden der Benachrichtigung angegeben. Der Standardwert beträgt 10.
- **Time-out des wiederholten Sendeversuchs**. Hier wird die Zeitspanne in Sekunden angegeben, die gewartet werden soll, bevor eine Benachrichtigung erneut versendet wird. Der Standardwert beträgt 300 Sekunden.
- **Workstation**. Hier wird die ID der Workstation angegeben, an die Benachrichtigungen versendet werden sollen. Die ID der Workstation wird in den Eigenschaften der Workstation angezeigt.

- **Speicherzeit der E-Mail**. Hier wird der Zeitraum angegeben, in dem eine erhaltene Benachrichtigung aufbewahrt werden soll. Der Standardwert beträgt 1 Tag. Wenn der angegebene Aufbewahrungszeitraum überschritten ist, wird die Benachrichtigung als veraltet gekennzeichnet und entsprechend der Aufgabe **Alte Nachrichten löschen** in den Einstellungen des **Servers** gelöscht.
- **Testnachricht senden**. Diese Option gibt an, dass eine Testbenachrichtigung entsprechend den festgelegten Einstellungen des Benachrichtigungssystems gesendet werden soll. Der Text einer Testbenachrichtigung kann in der jeweiligen Vorlage angegeben werden.

E-Mail-Benachrichtigungen

Um E-Mail-Benachrichtigungen versenden zu können, legen Sie die folgenden Einstellungen fest:

- **Anzahl der erneuten Sendevorgänge**. Hier wird die Anzahl der Wiederholungsversuche nach einem Fehler beim Senden der Benachrichtigung angegeben. Der Standardwert beträgt 10.
- **Time-out des wiederholten Sendeversuchs**. Hier wird die Zeitspanne in Sekunden angegeben, die gewartet werden soll, bevor eine Benachrichtigung erneut versendet wird. Der Standardwert beträgt 300 Sekunden.
- **E-Mail-Adresse des Absenders**. Hier wird die E-Mail-Adresse angegeben, die als Absender für E-Mail-Benachrichtigungen verwendet werden soll.
- **E-Mail-Adressen der Empfänger**. Hier werden die E-Mail-Adressen der Empfänger von Benachrichtigungen angegeben. In jedes Feld kann nur eine E-Mail-Adresse eingegeben werden. Um ein weiteres Feld hinzuzufügen, klicken Sie auf . Um ein Feld zu entfernen, klicken Sie auf .
- Geben Sie im Bereich **Einstellungen des SMTP-Servers** die folgenden Parameter an:
  - **Adresse**. Geben Sie hier die Adresse des SMTP-Servers an, der zum Versand von E-Mails verwendet werden soll.
  - **Port**. Geben Sie hier den Port des SMTP-Servers an, der zum Versand von E-Mails verwendet werden soll.
  - **Benutzer**, **Passwort**. Geben Sie hier den Namen und das Passwort vom Benutzer des SMTP-Servers an, wenn eine Autorisierung auf dem SMTP-Server erforderlich ist.
  - Aktivieren Sie das Kontrollkästchen **STARTTLS-Verschlüsselung**, um die *STARTTLS*-Verschlüsselung des Datenverkehrs beim Versand von E-Mail-Benachrichtigungen zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **SSL-Verschlüsselung**, um die *SSL*-Verschlüsselung des Datenverkehrs beim Versand von E-Mail-Benachrichtigungen zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **CRAM-MD5-Authentifizierung verwenden**, um die *CRAM-MD5*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **DIGEST-MD5-Authentifizierung verwenden**, um die *DIGEST-MD5*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **Übliche Authentifizierung verwenden**, um die *Plaintext*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **LOGIN-Authentifizierung verwenden**, um die *LOGIN*-Authentifizierung auf dem E-Mail-Server zu verwenden.
  - Aktivieren Sie das Kontrollkästchen **Richtigkeit des SSL-Zertifikats des Servers überprüfen**, um das SSL-Zertifikat des Servers auf Richtigkeit zu überprüfen.
  - Aktivieren Sie das Kontrollkästchen **Testbetrieb**, um SMTP-Sitzungen zu protokollieren.**Testnachricht senden**. Diese Option gibt an, dass eine Testbenachrichtigung entsprechend den festgelegten Einstellungen des Benachrichtigungssystems gesendet werden soll. Der Text einer Testbenachrichtigung kann in der jeweiligen Vorlage angegeben werden.

Benachrichtigungen über das SNMP-Protokoll

Um Benachrichtigungen über das SNMP-Protokoll versenden zu können, legen Sie die folgenden Einstellungen fest:

- **Anzahl der erneuten Sendevorgänge**. Hier wird die Anzahl der Wiederholungsversuche nach einem Fehler beim Senden der Benachrichtigung angegeben. Der Standardwert beträgt 10.
- **Time-out des wiederholten Sendeversuchs**. Hier wird die Zeitspanne in Sekunden angegeben, die gewartet werden soll, bevor eine Benachrichtigung erneut versendet wird. Der Standardwert beträgt 300 Sekunden.
- **Empfänger**. Hier wird die Entität angegeben, die SNMP-Anforderungen empfanden soll. In ein Feld kann nur ein Empfänger eingegeben werden. Um ein weiteres Feld hinzuzufügen, klicken Sie auf . Um ein vorhandenes Feld zu entfernen, klicken Sie auf .
- **Absender**. Hier wird die Entität angegeben, die SNMP-Anforderungen senden soll. Standardmäßig wird `"localhost"` für Windows und `""` für UNIX-basierte Betriebssysteme verwendet.
- **Gemeinschaft**. Hier wird die SNMP-Community oder der Kontext angegeben. Standardmäßig wird `public` verwendet.
- **Testnachricht senden**. Diese Option gibt an, dass eine Testbenachrichtigung entsprechend den festgelegten Einstellungen des Benachrichtigungssystems gesendet werden soll. Der Text einer Testbenachrichtigung kann in der jeweiligen Vorlage angegeben werden.

Push-Benachrichtigungen

Um Push-Benachrichtigungen an das **Dr.Web mobile Verwaltungscenter** zu versenden, legen Sie die folgenden Einstellungen fest:

- **Anzahl der erneuten Sendevorgänge**. Hier wird die Anzahl der Wiederholungsversuche nach einem Fehler beim Senden der Benachrichtigung angegeben. Der Standardwert beträgt 10.
- **Time-out des wiederholten Sendeversuchs**. Hier wird die Zeitspanne in Sekunden angegeben, die gewartet werden soll, bevor eine Benachrichtigung erneut versendet wird. Der Standardwert beträgt 300 Sekunden.
- **Testnachricht senden**. Diese Option gibt an, dass eine Testbenachrichtigung entsprechend den festgelegten Einstellungen des Benachrichtigungssystems gesendet werden soll. Der Text einer Testbenachrichtigung kann in der jeweiligen Vorlage angegeben werden.

Benachrichtigungen über den Windows-Nachrichtendienst

Das auf dem Windows Nachrichtendienst basierende Benachrichtigungssystem kann nur unter Windows-Betriebssystemen betrieben werden, die den Windows-Nachrichtendienst (Net Send) unterstützten.

Der Windows-Nachrichtendienst entfällt ab Windows Vista.

Um Benachrichtigungen über den Windows-Nachrichtendienst versenden zu können, legen Sie die folgenden Einstellungen fest:

- **Anzahl der erneuten Sendevorgänge**. Hier wird die Anzahl der Wiederholungsversuche nach einem Fehler beim Senden der Benachrichtigung angegeben. Der Standardwert beträgt 10.
- **Time-out des wiederholten Sendeversuchs**. Hier wird die Zeitspanne in Sekunden angegeben, die gewartet werden soll, bevor eine Benachrichtigung erneut versendet wird. Der Standardwert beträgt 300 Sekunden.

- **Empfänger**. Hier werden die Namen der Rechner angegeben, an die Benachrichtigungen versendet werden. In ein Feld kann nur ein Rechnername eingegeben werden. Um ein weiteres Feld hinzuzufügen, klicken Sie auf . Um ein vorhandenes Feld zu entfernen, klicken Sie auf .
- **Testnachricht senden**. Diese Option gibt an, dass eine Testbenachrichtigung entsprechend den festgelegten Einstellungen des Benachrichtigungssystems gesendet werden soll. Der Text einer Testbenachrichtigung kann in der jeweiligen Vorlage angegeben werden.

7.7.2. Benachrichtigungen der Web-Konsole

Über das **Verwaltungscenter** können Sie Benachrichtigungen, die mit der Sendemethode **Web-Konsole** gesendet wurden, ansehen und verwalten (diese Sendemethode wird im Abschnitt Benachrichtigungskonfiguration beschrieben).

So verwalten Sie Benachrichtigungen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Benachrichtigungen der Web-Konsole**. Die Liste mit den an die **Web-Konsole** gesendeten Benachrichtigungen wird angezeigt.
2. Um eine Benachrichtigung anzusehen, klicken Sie auf die jeweilige Zeile der Tabelle. Das Fenster mit dem Text der Benachrichtigung wird geöffnet. Die Benachrichtigung wird dabei automatisch als gelesen markiert.
3. Um die Liste mit Benachrichtigungen zu verwalten, verwenden Sie die folgenden Elemente:

   a) Allgemeine Elemente der Symbolleiste dienen zur Verwaltung des Benachrichtigungsbereichs. Diese Elemente sind jederzeit auf der Symbolleiste verfügbar.

Tabelle 7-6: Symbolleistenelemente zur Verwaltung von Benachrichtigungen der Web-Konsole

Einstellung		Aktion
Schweregrad	**Maximal**	Nur Benachrichtigungen mit dem Schweregrad **Maximal** werden angezeigt.
	Hoch	Nur Benachrichtigungen mit dem Schweregrad **Noch** oder **Maximal** werden angezeigt.
	Mittelmäßig	Nur Benachrichtigungen mit einem Schweregrad von **Mittelmäßig** bis **Maximal** werden angezeigt.
	Niedrig	Nur Benachrichtigungen mit einem Schweregrad von **Niedrig** bis **Maximal** werden angezeigt.
	Minimal	Nur Benachrichtigungen mit einem Schweregrad von **Minimal** bis **Maximal** werden angezeigt.
Quelle	**Agent**	Nur Benachrichtigungen über Ereignisse auf Workstations werden angezeigt.
	Server	Nur Benachrichtigungen über Ereignisse auf dem **Server** werden angezeigt.

Benachrichtigungen, die innerhalb eines Zeitraums empfangen wurden, können über einen der folgenden Wege angezeigt werden:

- Wählen Sie auf der Symbolleiste in der Dropdown-Liste einen der vorgegebenen Zeiträume.
- Wählen Sie in den Dropdown-Kalendern das Anfangsdatum und Enddatum des gewünschten Zeitraums.

Sobald alle erforderlichen Änderungen vorgenommen wurden, klicken Sie auf **Aktualisieren**, um die Benachrichtigungen entsprechend den von Ihnen angegebenen Einstellungen anzeigen zu lassen.

b) Um einzelne Benachrichtigungen zu verwalten, aktivieren Sie die Kontrollkästchen neben den benötigten Benachrichtigungen oder das im Tabellentitel, falls alle Benachrichtigungen in der Liste ausgewählt werden sollen. Die Elemente zur Verwaltung von ausgewählten Benachrichtigungen werden dabei auf der Symbolleiste verfügbar.

Benachrichtigungen löschen – alle ausgewählten Benachrichtigungen endgültig löschen.

Benachrichtigungen als bereits gelesen markieren – alle ausgewählten Benachrichtigungen als gelesen markieren.

c) Aktivieren Sie in der Liste von Benachrichtigungen das Symbol **Benachrichtigung ohne automatisches Löschen speichern** neben den Benachrichtigungen, die nach dem Ablauf des Aufbewahrungszeitraums automatisch nicht gelöscht werden sollen (der Aufbewahrungszeitraum für Benachrichtigungen wird vor dem Versand im Bereich Benachrichtigungskonfiguration in den Einstellungen für die Sendemethode **Web-Konsole** festgelegt). Solche Benachrichtigungen bleiben gespeichert, bis Sie diese im Bereich **Benachrichtigungen der Web-Konsole** manuell löschen oder das Symbol neben diesen Benachrichtigungen deaktivieren.

7.7.3. Nicht abgesendete Benachrichtigungen

Das **Verwaltungscenter** ermöglicht die Nachverfolgung und Verwaltung von Administrator-Benachrichtigungen, die anhand der im Bereich Benachrichtigungskonfiguration festgelegten Einstellungen nicht gesendet werden konnten.

So lassen Sie nicht gesendete Benachrichtigungen anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Nicht abgesendete Benachrichtigungen**. Die Liste mit nicht gesendeten Benachrichtigungen des **Servers** wird angezeigt.
2. In die Liste mit nicht gesendeten Benachrichtigungen werden diejenigen Benachrichtigungen verschoben, die an die Empfänger zwar nicht gesendet werden konnten, aber doch die festgelegte Anzahl der erneuten Sendeversuche noch nicht erreicht wurde.
3. Die Tabelle mit nicht gesendeten Benachrichtigungen enthält die folgenden Informationen:
   - **Benachrichtigung**. Hier wird der Name einer Standardbenachrichtigung angezeigt.
   - **Überschrift**. Hier wird der Name des Benachrichtigungsprofils angezeigt, dessen Einstellungen zum Versand der Benachrichtigung verwendet werden.
   - **Anzahl der ausstehenden Sendeversuche**. Hier wird die Anzahl der verbleibenden erneuten Sendeversuche angezeigt. Die Anzahl der erneuten Sendeversuche wird im Bereich Benachrichtigungskonfiguration beim Konfigurieren von Benachrichtigungen festgelegt. Nachdem eine Benachrichtigung einmal versendet wurde, kann die Anzahl der erneuten Sendeversuche für diese Benachrichtigung nicht geändert werden.
   - **Zeit des nächsten Sendeversuchs**. Hier werden das Datum und die Uhrzeit des nächsten erneuten Sendeversuchs angezeigt. Das Zeitintervall, mit dem eine Benachrichtigung erneut gesendet werden soll, wird im Bereich Benachrichtigungskonfiguration beim Konfigurieren von Benachrichtigungen festgelegt. Nachdem eine Benachrichtigung einmal versendet wurde, kann das Zeitintervall für diese Benachrichtigung nicht geändert werden.
   - **Empfänger**. Hier wird die Adresse des Empfängers der Benachrichtigung angezeigt.
   - **Fehler**. Hier wird das Problem angezeigt, das zu Fehler beim Senden der Benachrichtigung geführt hat.
4. So verwalten Sie nicht gesendete Benachrichtigungen
   a) Aktivieren Sie die Kontrollkästchen neben den gewünschten Benachrichtigungen oder das Kontrollkästchen in der Überschrift, um alle Benachrichtigungen auszuwählen.
   b) Auf der Symbolleiste sind die folgenden Schaltflächen verfügbar:

      Erneut senden – ausgewählte Benachrichtigungen sofort versenden. Die Benachrichtigung wird dabei außerhalb der Reihenfolge sofort versendet. Ein fehlgeschlagener Sendeversuch verringert die Anzahl der erneuten Sendeversuche um 1. Die Zeit des nächsten Sendeversuchs wird anhand des im Bereich Benachrichtigungskonfiguration festgelegten Zeitintervalls ermittelt.

      Entfernen – alle ausgewählten nicht gesendeten Benachrichtigungen endgültig löschen.

5. Nicht gesendete Benachrichtigungen werden in den folgenden Fällen aus der Liste entfernt:
   a) Benachrichtigung wurde an den Empfänger erfolgreich zugestellt.
   b) Benachrichtigung wurde vom Administrator manuell oder mit der sich auf der Symbolleiste befindenden Schaltfläche **Entfernen** gelöscht.
   c) Die Anzahl der erneuten Sendeversuche wurde erreicht, und die Benachrichtigung wurde nicht versendet.
   d) Im Bereich Benachrichtigungskonfiguration wurde das Benachrichtigungsprofil gelöscht, dessen Einstellungen zum Versand der Benachrichtigungen verwendet wurden.

7.8. Dr.Web Server-Repository verwalten

Das *Repository* des **Dr.Web Servers** dient zur Speicherung von Originalkopien der Software sowie zu deren Aktualisierung über die Server des **Globalen Update-Systems.**

Das Repository enthält Dateisätze, die als *Produkte* bezeichnet werden. Jedes Produkt befindet sich in einem Unterverzeichnis des Verzeichnisses `repository`, das im Verzeichnis `var` angelegt wird. Dieses Verzeichnis wird standardmäßig als Unterverzeichnis im Stammverzeichnis des **Servers** erstellt. Jedes Produkt im Repository wird individuell gehandhabt.

Zur Steuerung des Update-Vorgangs verwendet das Repository sog. *Revisionen*. Eine Revision ist ein aktueller Zustand von Produktdateien (darunter Dateinamen und Prüfsummen) zu gewissem Zeitpunkt. Jede Revision wird eindeutig gekennzeichnet.

Das Repository synchronisiert Revisionen eines Produkts in die folgenden Richtungen:

a) An den **Dr.Web Server** von der Webseite zur Aktualisierung des Produkts (über das HTTP-Protokoll).
b) Zwischen verschiedenen **Dr.Web Servern**, wenn das Netzwerk aus mehreren Servern besteht (entsprechend der festgelegten Richtlinie für die Synchronisierung).
c) Vom **Dr.Web Server** an die Workstations.

Das Repository ermöglicht dem Administrator des Antivirus-Netzwerks, die folgenden Einstellungen festzulegen:

- Liste von Aktualisierungswebseiten bei Vorgängen des Typs **a)**.
- Einschränkungen bezüglich Produkten, welche die Synchronisierung des Typs **a)** benötigen (dadurch kann der Benutzer nur für ihn relevante Änderungen bestimmter Produktkategorien verfolgen).
- Einschränkungen bezüglich Produktkomponenten, welche die Synchronisierung des Typs **c)** benötigen (dadurch kann der Benutzer entscheiden, welche Komponenten installiert werden sollen).
- Wechsel zu neuen Revisionen (dadurch können Produkte vor dem Rollout getestet werden).
- Implementierung eigener Software-Lösungen in ein Produkt.
- Selbständige Entwicklung neuer Produkte: Eigene Produkte können auch mit synchronisiert werden.

Zum aktuellen Lieferumfang gehören die folgenden Produkte:

- **Dr.Web Server**
- **Dr.Web Agents** (Software des **Agents**, Antivirensoftware der Workstation für das jeweilige Betriebssystem)
- **Dr.Web Proxy-Server**
- **Dr.Web** Virendatenbanken
- Datenbanken von **SpIDer Gate**
- Datenbanken vom **Dr.Web Anti-Spam**
- Firmennachrichten von **Doctor Web**

7.8.1. Status des Repository

So überprüfen Sie den aktuellen Zustand des Repository oder aktualisieren Sie Komponenten des Antivirus-Netzwerks

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Status des Repository**.
2. Im angezeigten Fenster werden die Liste der Repository-Produkte, das Datum der aktuell verwendeten Revision, das Datum der zuletzt heruntergeladenen Revision und den aktuellen Zustand der Produkte angezeigt.
3. Zur Verwaltung des Repository-Inhalts verwenden Sie die folgenden Schaltflächen:
   - Klicken Sie auf **Auf Updates überprüfen**, um zu überprüfen, ob auf dem **GUS** Updates für alle Produkte verfügbar sind, oder vorhandene Updates vom **GUS** herunterzuladen.
   - Klicken Sie auf **Repository vom Laufwerk erneut herunterladen**, um die aktuelle Version des Repository von der Festplatte erneut zu laden.

   Beim Start lädt der **Server** den Inhalt des Repository in den Speicher. Wenn der Administrator beim Betrieb des **Servers** den Inhalt des Repository nicht über das **Verwaltungscenter** geändert hat, muss das Repository erneut geladen werden, damit die auf der Festplatte geladene Repository-Version verwendet werden kann. Das kann dann der Fall sein, wenn der Administrator den Inhalt des Repository mithilfe eines externen Dienstprogramms oder manuell aktualisiert hat.

7.8.2. Verschobene Aktualisierungen

Im Bereich **Verschobene Aktualisierungen** werden Produkte aufgelistet, für die im Bereich **Detaillierte Konfiguration des Repository** → *<Produkt>* → Verschobene Aktualisierungen Updates vorübergehend deaktiviert wurden. Eine ausstehende Revision gilt als *gesperrt*.

Die Tabelle von gesperrten Produkten enthält die folgenden Informationen:

- **Repository-Ordner**. Hier wird der Name vom Repository-Verzeichnis des gesperrten Produkts angezeigt:
  - 10-drwgatedb – Datenbanken von **SpIDer Gate**,
  - 10-drwspamdb – Datenbanken von **AntiSpam**,
  - 20-drwagent – **Dr.Web Agent** für Windows,
  - 20-drwandroid – **Dr.Web Agent** für Android,
  - 20-drwcs – **Dr.Web Server**,
  - 20-drwunix – **Dr.Web Agent** für UNIX,
  - 80-drwnews – Firmennachrichten von **Doctor Web**.
- **Aktualisierung** – Nummer der gesperrten Revision.
- **Verschoben bis** – Zeit, bis zu der keine Aktualisierung des Produkts erfolgen soll.

Durch Anklicken einer Zeile der Tabelle von gesperrten Produkten wird eine weitere Tabelle geöffnet, die detaillierte Informationen zur gesperrten Revision dieses Produkts enthält.

Die Funktion der ausstehenden Aktualisierung bietet Ihnen die Möglichkeit, die Verteilung der letzten Revision an alle Workstations vorübergehend zu verbieten. Das macht Sinn, wenn Sie eine Revision zunächst auf einigen Workstations testen wollen.

Um Funktionen der ausstehenden Aktualisierung zu verwenden, führen Sie die Aktionen aus, die im Abschnitt **Detaillierte Konfiguration des Repository** → Verschobene Aktualisierungen beschrieben werden.

So verwalten Sie ausstehende Aktualisierungen

1. Aktivieren Sie das Kontrollkästchen neben den Produkten, für die ausstehende Aktualisierungen konfiguriert werden sollen. Um alle Produkte auszuwählen, aktivieren Sie das Kontrollkästchen in der Überschrift der Tabelle gesperrter Produkte.
2. Wählen Sie auf der Symbolleiste die gewünschte Aktion:

   Sofort ausführen – Updates für das Produkt erneut aktivieren, die Revision in die Liste von Revisionen aufnehmen und an Workstations entsprechend der allgemeinen Prozedur verteilen.

   Aktualisierung zurücksetzen – Updates für das Produkt erneut aktivieren und die Revision verbieten. Updates können dann erneut über das **GUS** heruntergeladen werden. Die freigegebene Revision wird aus der Liste der Revisionen des Produkts entfernt. Wenn eine neue Revision bereitgestellt wird, wird die freigegebene Revision auch von der Festplatte entfernt.

   Zeitintervall für Verzögerung von Updates ändern – den Zeitraum angeben, in dem die Revision des Produkts verzögert werden soll. Die Revisionssperrzeit läuft ab dem Erhalt der Revision vom **GUS**.
3. Wenn Sie keine Aktionen für die Entsperrung des gesperrten Produkts durchgeführt haben, wird die Revision nach dem Ablauf des in der Liste **Updates-Verzögerungsintervall** festgelegten Zeitraums automatisch entsperrt und in die Liste von Revisionen aufgenommen sowie an Workstations entsprechend der allgemeinen Prozedur verteilt.

7.8.3. Allgemeine Konfiguration des Repository

Der Bereich **Allgemeine Konfiguration des Repository** öffnet das Fenster mit den Einstellungen für die Verbindung mit dem **GUS** und Aktualisierung des Repository für alle Produkte.

So bearbeiten Sie die Repository-Konfiguration

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster den Punkt des Verwaltungsmenüs **Allgemeine Konfiguration des Repository**.
3. Legen Sie alle unterstehenden Einstellungen für die Verbindung mit dem **GUS** fest.
4. Wenn Sie beim Bearbeiten der Einstellungen alle vorgenommen Änderungen verwerfen wollen, verwenden Sie die folgenden Schaltflächen auf der Symbolleiste:

   Alle Parameter mit den ursprünglichen Werten wiederherstellen. Diese Option gibt an, dass ursprüngliche Werte aller Einstellungen des Bereichs wiederhergestellt werden sollen. Um diese Aktion auf einzelne Einstellungen anzuwenden, verwenden Sie die Schaltfläche neben der gewünschten Einstellung.

   Defaultparameter wiederherstellen. Diese Option gibt an, dass die in der Konfigurationsdatei des **Servers** gespeicherten Werte für alle Einstellungen des Bereichs wiederhergestellt werden sollen. Um diese Aktion auf einzelne Einstellungen anzuwenden, verwenden Sie die Schaltfläche neben der gewünschten Einstellung.
5. Klicken Sie auf der Symbolleiste eine der folgenden Schaltflächen an:
   - **Speichern und erneut synchronisieren**. Diese Option gibt an, dass alle vorgenommen Änderungen übernommen werden sollen und das Repository entsprechend den neuen Einstellungen vom **GUS** aktualisiert werden soll.
   - **Speichern und vom Laufwerk erneut herunterladen**. Diese Option gibt an, dass alle vorgenommenen Änderungen übernommen werden sollen, ohne dass das Repository über das **GUS** aktualisiert wird. Die aktuelle Version des Repository wird dabei von der Festplatte erneut geladen (s. dazu Status des Repository).

Dr.Web GUS konfigurieren

Auf der Registerkarte **Dr.Web GUS** können Sie die Einstellungen für die Verbindung mit dem **Globalen Update-System** festlegen.

So bearbeiten Sie die Einstellungen für die Verbindung mit dem GUS

- **Basis-URI** – Verzeichnis auf den Servern des GUS, in dem Updates für Produkte von **Dr.Web** gespeichert werden.
- Aktivieren Sie das Kontrollkästchen **CDN verwenden**, um Content Delivery Network beim Herunterladen des Repository zuzulassen.
- Aktivieren Sie das Kontrollkästchen **SSL verwenden**, um das Repository mittels gesicherter SSL-Verbindung zu laden.

  Wählen Sie dazu in der Liste **Akzeptierte Zertifikate** die SSL-Zertifikate, die automatisch akzeptiert werden sollen.

- Ändern Sie bei Bedarf die Liste der **GUS**-Server, von denen das Repository aktualisiert werden soll. Wechseln Sie dafür zum Bereich **Liste der Server im globalen Dr.Web Aktualisierungssystem**:
  - Um einen **GUS**-Server in die Liste der Update-Server aufzunehmen, klicken Sie auf und geben Sie im Feld die Adresse eines neuen **GUS**-Servers an.
  - Um einen **GUS**-Server aus der Liste zu entfernen, klicken Sie auf neben dem zu entfernenden Server.
  - Alle **GUS**-Server werden in der Reihenfolge aufgelistet, in der sie vom **Dr.Web Server** Anforderungen beim Update des Repository erhalten. Um die Reihenfolge der **GUS**-Server zu ändern, ziehen Sie die Server-Zeile an die gewünschte Position in der Liste.

  Bei der Installation des **Dr.Web Servers** enthält die Liste nur Update-Server von **Doctor Web**. Sie können bei Bedarf eigene Update-Quellen einrichten und sie zur Liste von Update-Server hinzufügen.

Update des Dr.Web Servers konfigurieren

Die Aktualisierung des Repository für die Software des **Agents** und Antivirenpakets wird für jedes Betriebssystem individuell konfiguriert:

- Geben Sie auf der Registerkarte **Dr.Web für Windows** an, ob alle auf Workstations unter Windows installierten Komponenten oder nur Virendatenbanken aktualisiert werden sollen.
- Geben Sie auf der Registerkarte **Dr.Web Agent für Unix** an, für welche Unix-artigen Betriebssysteme die auf Workstations installierten Komponenten aktualisiert werden sollen.

Um keine Updates vom **GUS** für den **Agent für UNIX** zu erhalten, wechseln Sie zum Bereich **Detaillierte Konfiguration des Repository** und dann zum Punkt **Dr.Web Agent für UNIX**. Aktivieren Sie auf der Registerkarte **Synchronisierung** das Kontrollkästchen **Produktaktualisierung deaktivieren**.

Update des Dr.Web Servers konfigurieren

Geben Sie auf der Registerkarte **Dr.Web Server** an, für welche Betriebssysteme Dateien des **Servers** aktualisiert werden sollen:

- Um Updates für den **Server** unter einem unterstützten Betriebssystemen zu erhalten, aktivieren Sie das Kontrollkästchen **Alle im GUS vorhandenen Plattformen aktualisieren**.
- Um Updates für den **Server** unter einem bestimmten Betriebssystem zu erhalten, aktivieren Sie das Kontrollkästchen neben dem gewünschten Betriebssystem.

Um keine Updates vom **GUS** für den **Server** zu erhalten, wechseln Sie zum Bereich **Detaillierte Konfiguration des Repository** und dann zum Punkt **Dr.Web Server**. Aktivieren Sie auf der Registerkarte **Synchronisierung** das Kontrollkästchen **Produktaktualisierung deaktivieren**.

Unternehmensnachrichten von Doctor Web

Wählen Sie auf der Registerkarte **Unternehmensnachrichten von Doctor Web** Ihre gewünschten Sprachen für Newsfeed aus.

Im Bereich Präferenzen → **Abonnement** können Sie einzelne Nachrichten-Kategorien abonnieren.

Sie können die aktuellsten Firmennachrichten von **Doctor Web** im Hauptmenü des **Verwaltungscenters** **Hilfe** → **News** jederzeit lesen.

Sprachen des Dr.Web Agenten für Windows

Geben Sie auf der Registerkarte **Sprachen des Dr.Web Agenten für Windows** Sprachen für die Oberfläche des **Agents** und Antivirenpakets für Windows an, die über das **GUS** heruntergeladen werden sollen.

7.8.4. Detaillierte Konfiguration des Repository

Der Bereich **Detaillierte Konfiguration des Repository** ermöglicht Ihnen, Revisionen für einzelne Repository-Produkte individuell zu konfigurieren.

So bearbeiten Sie die Repository-Konfiguration

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im Unterbereich des Verwaltungsmenüs **Detaillierte Konfiguration des Repository** den Punkt, der dem zu bearbeitenden Produkt einspricht.
3. Legen Sie alle erforderlichen Repository-Einstellungen für das gewählte Produkt. Diese Einstellungen werden nachfolgend beschrieben.
4. Klicken Sie auf der Symbolleiste auf **Speichern und vom Laufwerk erneut herunterladen**, um alle vorgenommenen Änderungen zu übernehmen. Die aktuelle Version des Repository wird dabei von der Festplatte erneut geladen (s. dazu Status des Repository).

Liste der Revisionen

Auf der Registerkarte **Liste der Aktualisierungen** finden Sie Informationen zu allen Revisionen des Produkts, die auf dem **Server** verfügbar sind.

Die Tabelle von Revisionen enthält die folgenden Spalten:

Spaltenname	Beschreibung des Inhalts
Verteilt	Die automatische Markierung in dieser Spalte bestimmt den Zustand der Produktrevision. In der Spalte werden zwei Markierungen verwendet: – *Verteilte Revision*. Die Markierung gibt an, dass diese Revision für das Update der **Agents** und Antivirensoftware auf Workstations verwendet wird. Eine zu verteilende Revision wird folgendermaßen ausgewählt:

Spaltenname	Beschreibung des Inhalts
	1. Eine Revision mit der Markierung in der Spalte **Aktuell** wird verteilt. Nur eine Revision kann auf diese Weise markiert werden. Für das Produkt **Dr.Web Agent für Windows** kann eine Revision, die früher als die zum aktuellen Zeitpunkt zu verteilende Revision erhalten wurde, nicht markiert werden. 2. Wenn in der Spalte **Aktuell** keine Revision markiert wurde, wird die letzte Revision, die durch die Markierung in der Spalte **Gespeichert** gekennzeichnet wurde, verteilt. 3. Wenn in den Spalten **Aktuell** und **Gespeichert** keine Revision markiert wurde, wird die letzte Revision verteilt. Die automatische Markierung weist immer auf die zu verteilende Revision hin. – *Gesperrte Revision*. Diese Revision wird nicht verteilt, keine neuen Revisionen werden vom **Server** heruntergeladen. Mehr dazu finden Sie im Abschnitt Verschobene Aktualisierungen. Wenn eine gesperrte Revision vorhanden ist, wird eine zu verteilende Revision folgendermaßen gewählt: 1. Wenn die Markierung in der Spalte **Aktuell** vorhanden ist, wird die aktuelle Revision an Workstations verteilt. 2. Wenn die Markierung in der Spalte **Aktuell** nicht vorhanden ist, wird an Workstations die der gesperrten Revision vorangehende Revision verteilt.
Aktuell	Fügen Sie die Markierung hinzu, um die Produktrevision anzugeben, die für das Update der **Agents** und Antivirensoftware auf Workstations verwendet wird. Nur eine aktuelle Revision kann ausgewählt werden. Alternativ kann keine Markierung für die aktuelle Revision hinzugefügt werden.
Gespeichert	Fügen Sie die Markierung hinzu, um die Revision beim automatischen Aufräumen beizubehalten. Die Markierung kann mehreren Revisionen gleichzeitig hinzugefügt werden. Alternativ kann keine Markierung hinzugefügt werden. **Server** speichert eine bestimmte Anzahl von Revision auf der Festplatte. Diese Anzahl kann auf der Registerkarte **Synchronisierung** festgelegt werden. Wenn die maximal zulässige Anzahl erreicht wird, wird die älteste Revision gelöscht, damit die neue über das **GUS** heruntergeladene Revision gespeichert werden kann. Nicht gelöscht werden beim automatischen Aufräumen des Repository die folgenden Revisionen: • Revisionen, die durch die Markierung in der Spalte **Gespeichert** gekennzeichnet wurden. • Revision, die durch die Markierung in der Spalte **Aktuell** gekennzeichnet wurde. Wenn eine Revision stabil ist, kann sie als gespeichert gekennzeichnet werden: Falls vom **GUS** eine nicht stabile Revision bereitgestellt wird, können Sie auf die vorherige (stabile) Revision zurückgreifen.
Aktualisierung	Hier wird das Datum angegeben, an dem eine Produktrevision erhalten wurde. Wenn es sich um eine gesperrte Revision handelt, wird in dieser Spalte ihr Sperrstatus angezeigt.

Synchronisierung

Auf der Registerkarte **Synchronisierung** können Sie die Einstellungen festlegen, anhand derer das Repository des **Servers** über das **GUS** aktualisiert werden soll:

- Wählen Sie in der Dropdown-Liste **Anzahl der gespeicherten Revisionen** die Anzahl von Revisionen, die temporär auf der Festplatte gespeichert werden sollen. Dazu zählen nicht die Revisionen, die mindestens in einer Spalte der Registerkarte **Liste der Revisionen** markiert sind. Wenn eine neue Revision verfügbar ist und die maximal zulässige Anzahl an Produktrevisionen erreicht wurde, wird die älteste Revision gelöscht. Die als **Aktuell**, **Gespeichert** und **Verteilt** markierten Revisionen können nicht gelöscht werden.
- Aktivieren Sie das Kontrollkästchen **Produktaktualisierung deaktivieren**, damit das Produkt über das **GUS** nicht aktualisiert wird. **Agents** werden dabei bis auf die aktuelle Version auf dem **Server** (oder entsprechend der Prozedur für die Verteilung von Revisionen) aktualisiert.

Für einige Produkte sind folgende Einstellungen verfügbar:

- Aktivieren Sie das Kontrollkästchen **Nur folgende Dateien aktualisieren**, damit nur unten angegebene Dateien über das **GUS** aktualisiert werden.
- Aktivieren Sie das Kontrollkästchen **Nur folgende Dateien nicht aktualisieren**, damit nur unten angegebene Dateien über das **GUS** nicht aktualisiert werden.

  Bei der Angabe der Dateien können Sie reguläre Ausdrücke verwenden.

  Wenn beide Kontrollkästchen aktiviert sind, werden die zu aktualisierenden Dateien folgendermaßen ausgewählt:

  1. In der vollständigen Liste der Dateien werden nur diejenigen Dateien gewählt, die in der Liste **Nur folgende Dateien aktualisieren** angegeben wurden.
  2. Aus der Liste, die im Schritt 1 generiert wurde, werden alle Dateien entfernt, die in der Liste **Nur folgende Dateien nicht aktualisieren** angegeben wurden.
  3. Über das **GUS** werden nur diejenigen Dateien aktualisiert, die nach dem Schritt 2 übrig geblieben sind.

Benachrichtigungen

Auf der Registerkarte **Benachrichtigungen** können Sie Benachrichtigungen über Updates des Repository festlegen:

- Aktivieren Sie das Kontrollkästchen **Nur über folgende Dateien nicht benachrichtigen**, damit keine Benachrichtigungen nur über die in der Liste unten angegebenen Dateien versendet werden.
- Aktivieren Sie das Kontrollkästchen **Nur über folgende Dateien benachrichtigen**, damit Benachrichtigungen nur über die in der Liste unten angegebenen Dateien versendet werden.

  Bei der Angabe der Dateien können Sie reguläre Ausdrücke verwenden.

Wenn keine Ausnahmelisten festgelegt wurden, werden alle Benachrichtigungen versendet, die auf der Seite Benachrichtigungskonfiguration aktiviert wurden.

Benachrichtigungen über Updates des Repository werden auf der Seite der Benachrichtigungskonfiguration im Unterbereich **Repository** konfiguriert.

Verschobene Aktualisierungen

Auf der Registerkarte **Verschobene Aktualisierungen** können Sie die Verteilung von Updates um einen bestimmten Zeitraum verschieben. Eine verschobene Revision gilt als *gesperrt*.

Diese Funktion bietet Ihnen die Möglichkeit, die Verteilung der letzten Revision an alle Workstations vorübergehend zu verbieten. Das macht Sinn, wenn Sie eine Revision zunächst auf einigen Workstations testen wollen.

So verwenden Sie die Funktion der verschobenen Aktualisierungen

1. Konfigurieren Sie verschobene Aktualisierungen für das zu sperrende Produkt wie unten beschrieben.
2. Um die letzte Revision nicht zu verteilen, legen Sie auf der Registerkarte Liste der Revisionen eine der vorherigen Revisionen als aktuell fest.
3. Aktivieren Sie das Kontrollkästchen **Alle neuesten Updates erhalten** für die Gruppe von Workstations, an welche die letzte Revision verteilt werden soll. Wechseln Sie dafür zum Bereich **Antivirus-Netzwerk** → Updates für Workstations einschränken. An alle anderen Workstations wird die Revision verteilt, die Sie im Schritt 2 als aktuell markiert haben.
4. Die nächste über das **GUS** heruntergeladene Revision, welche die Bedingungen der Option **Nur Aktualisierungen der folgenden Dateien verschieben** erfüllt, wird gesperrt und um den in der Liste **Updates-Verzögerungsintervall** angegebenen Zeitraum verschoben.

So konfigurieren Sie verschobene Aktualisierungen

1. Aktivieren Sie das Kontrollkästchen **Updates verschieben**, um vorübergehend keine Updates für das Produkt über das **GUS** zu erhalten.
2. Wählen Sie in der Dropdown-Liste **Updates-Verzögerungsintervall** den Zeitraum, um den die Aktualisierung verschoben werden soll. Der Zeitraum läuft ab dem Erhalt von über das **GUS** heruntergeladenen Updates.
3. Aktivieren Sie bei Bedarf das Kontrollkästchen **Nur Aktualisierungen der folgenden Dateien verschieben**, um die Updates nicht zu verteilen, die unten angegebenen Masken entsprechende Dateien enthalten. Masken müssen mithilfe von regulären Ausdrücken angegeben werden.

   Wenn das Kontrollkästchen deaktiviert ist, werden alle über das **GUS** bezogenen Updates gesperrt.

So entsperren Sie eine Revision

- Klicken Sie auf der Registerkarte **Liste der Revisionen** auf **Sofort ausführen**, um Updates für das Produkt erneut zu aktivieren, die Revision in die Liste von Revisionen aufzunehmen und an Workstations entsprechend der allgemeinen Prozedur zu verteilen.
- Klicken Sie auf der Registerkarte **Liste der Revisionen** auf **Aktualisierung zurücksetzen**, um Updates für das Produkt erneut zu aktivieren und die Revision zu verbieten. Updates können dann erneut über das **GUS** heruntergeladen werden. Die entsperrte Revision wird von der Liste der Revisionen des Produkts entfernt. Wenn eine neue Revision bereitgestellt wird, wird die freigegebene Revision auch von der Festplatte entfernt.
- Nach dem Ablauf des in der Liste **Updates-Verzögerungsintervall** festgelegten Zeitraums wird die Revision automatisch entsperrt und in die Liste von Revisionen aufgenommen sowie an Workstations entsprechend der allgemeinen Prozedur verteilt.

Gesperrte Revisionen für alle Produkte werden im Bereich Verschobene Aktualisierungen gehandhabt.

7.8.5. Inhalt des Repository

Der Bereich **Inhalt des Repository** dient zur Anzeige und Verwaltung des aktuellen Inhalts vom Repository auf Verzeichnis- und Dateiebene.

Das Hauptfenster des Bereichs **Inhalt des Repository** enthält eine hierarchisch strukturierte Darstellung aller Verzeichnisse und Dateien der aktuellen Repository-Version und vorhandenen Revisionen aller Produkte.

Informationen zum Repository anzeigen

Um Informationen zu einem Repository-Objekt anzuzeigen, wählen Sie in der hierarchischen Baumstruktur des Repository-Inhalts das gewünschte Objekt. Die angezeigte Eigenschaftenleiste enthält die folgenden Informationen:

- Im Unterbereich **Ausgewählte Objekte** finden Sie detaillierte Informationen zum ausgewählten Objekt: **Typ**, **Größe** (nur für einzelne Dateien), **Erstellungsdatum** und **Änderungsdatum**.
- Im Unterbereich **Status des Repository** finden Sie allgemeine Informationen zu allen Objekten des Repository, darunter die aktuelle Liste von Objekten und das Datum ihrer letzten Aktualisierung.

Repository verwalten

Verwenden Sie zur Verwaltung des Repository-Inhalts die folgenden Schaltflächen auf der Symbolleiste:

Repository-Dateien in Archiv exportieren.

Archiv mit Repository-Dateien importieren.

Ausgewählte Objekte entfernen. Diese Option gibt an, dass die in der Baumstruktur des Repository-Inhalts gewählten Objekte endgültig gelöscht werden sollen.

Wenn der Inhalt des Repository geändert wurde, muss das Repository neu gestartet werden, damit der **Server** geänderte Daten verwenden kann.

Mehr dazu finden Sie unter Status des Repository.

Repository exportieren

So speichern Sie Repository-Dateien in einem ZIP-Archiv

1. Wählen Sie in der hierarchischen Baumstruktur des Repository-Inhalts ein Produkt, eine Produktrevision oder das gesamte Repository. Das gesamte Repository wird exportiert, wenn in der Baumstruktur kein Objekt ausgewählt oder der Wurzelknoten der Repository-Baumstruktur **Repository** gewählt wurde. Zur Mehrfachauswahl verwenden Sie die STRG oder UMSCHALTTASTE.

   Achten Sie beim Export des Repository auf die Typen der zu exportierenden Objekte:

   a) ZIP-Archive der Repository-Produkte. Diese Archive enthalten einen der folgenden Typen von Repository-Objekten:
      - Das gesamte Repository.
      - Das gesamte Produkt.
      - Einzelne gesamte Revision.

   Die beim Export dieser Objekte generierten Archive können über den Bereich **Inhalt des Repository** importiert werden. Namen dieser Archive haben das Präfix `repository_`.

   b) ZIP-Archive einzelner Repository-Dateien.

   Die beim Export einzelner Dateien und Verzeichnisse generierten Archive, die sich in der Baumstruktur unterhalb von den Objekten aus dem Punkt **a)** befinden, können über den Bereich **Inhalt des Repository** nicht importiert werden. Namen dieser Archive haben das Präfix `files_`.

   Solche Archive können als Sicherungskopien für die manuell zu ersetzenden Dateien verwenden werden. Die manuelle Ersetzung von Repository-Dateien ist nicht empfehlenswert. Zu diesem Zweck sollten Sie den Bereich **Inhalt des Repository** verwenden.

2. Klicken Sie auf der Symbolleiste auf **Repository-Dateien in Archiv exportieren**.

3. Der Pfad des zu speichernden ZIP-Archivs wird entsprechend den Einstellungen des Webbrowsers, in dem das **Verwaltungscenter** geöffnet wurde, festgelegt.

Repository importieren

So laden Sie Repository-Dateien aus einem ZIP-Archiv

1. Klicken Sie auf der Symbolleiste auf **Archiv mit Repository-Dateien importieren**.
2. Geben Sie im nächsten Fenster im Bereich **Datei wählen** das benötigte ZIP-Archiv an. Um die gewünschte Datei auszuwählen, klicken Sie auf .

   Importiert werden können nur diejenigen ZIP-Archive, die beim Export eines der folgenden Typen von Repository-Objekten generiert wurden:

   - Das gesamte Repository.
   - Das gesamte Produkt.
   - Einzelne gesamte Revision.

   Diese Archive haben das Präfix `repository_`.
3. Geben Sie im Bereich **Importeinstellungen** die folgenden Parameter an:
   - **Nur fehlende Revisionen hinzufügen**. Diese Option gibt an, dass nur in der aktuellen Repository-Version nicht enthaltene Revisionen hinzugefügt werden sollen. Alle anderen Revisionen bleiben unverändert.
   - **Repository komplett ersetzen**. Diese Option gibt an, dass das aktuelle Repository durch das zu importierende Repository komplett ersetzt werden soll.
   - Aktivieren Sie das Kontrollkästchen **Konfigurationsdateien importieren**, um beim Import des Repository Konfigurationsdateien mit zu importieren.
4. Klicken Sie auf **Importieren**, um den Import zu starten.

7.9. Zusätzliche Funktionen

7.9.1. Datenbankverwaltung

Datenbankverwaltung ermöglicht die Verwaltung der Datenbank, die der **Dr.Web Server** zum aktuellen Zeitpunkt verwendet.

Der Bereich **Allgemein** enthält folgende Parameter:

- Das Feld **Letzte Aktualisierung der Datenbank**. Hier wird das Datum der letzten Wartung der Datenbank angegeben.
- Liste der Befehle zur Wartung der Datenbank, darunter:
  - Befehle, die mit den Aufgaben des Dr.Web Server-Zeitplans identisch sind. Namen der Befehle entsprechen den Namen der Aufgaben im Bereich **Aktionen** des **Dr.Web Server-Aufgabenplaners** (diese Aufgaben sind in der Tabelle Typen und Parameter der Aufgaben detailliert beschrieben).
  - Der Befehl **Datenbankanalyse** dient zur Optimierung der Datenbank des **Servers** mithilfe des Befehls `analyse`.

So führen Sie Befehle zur Wartung der Datenbank aus

1. Aktivieren Sie die Kontrollkästchen neben den Befehlen, die ausgeführt werden sollen.

   Legen Sie bei Bedarf fest, in welchem Abstand die Datenbank des **Servers** bereinigt werden soll.
2. Klicken Sie auf **Jetzt anwenden**. Alle gewählten Befehle werden sofort ausgeführt.

Wenn Sie wollen, dass bestimmte Befehle (außer dem Befehl **Datenbankanalyse**) später oder regelmäßig ausgeführt werden, verwenden Sie den Dr.Web Server-Aufgabenplaner.

Folgende Schaltflächen auf der Symbolleiste können zur Verwaltung der Datenbank verwendet werden:

Import

Export

Sicherungskopie

Datenbank exportieren

So exportieren Sie Informationen aus der Datenbank in eine Datei

1. Klicken Sie auf der Symbolleiste auf **Export**.
2. Wählen Sie im Dialogfeld eine der folgenden Optionen aus:
   - **Die Datenbank komplett exportieren**, um alle Informationen aus der Datenbank in einem GZ-Archiv zu speichern. Die auf diese Weise generierte XML-Datei ist identisch mit der Exportdatei, die beim Start der ausführbaren Datei des **Servers** über den Schalter `xmlexportdb` erstellt wird. Diese Exportdatei kann dann beim Start der ausführbaren Datei des **Servers** über den Schalter `xmlimportdb` importiert werden.
     Weitere Informationen zu diesen Befehlen finden Sie im Dokument **Anhänge** unter H3.3. Befehle für die Datenbankverwaltung).
   - **Informationen zu Stationen und Gruppen exportieren**, um Informationen zu Objekten des Antivirus-Netzwerks in einem ZIP-Archiv zu speichern. In einer speziellen Datei werden dabei alle Informationen zu Gruppen von Workstations und Konten der Workstations des Antivirus-Netzwerks gespeichert, das durch den **Server** gewartet wird. Die exportierte Datei enthält folgende Daten zu Workstations: Eigenschaften, Konfiguration der Komponenten, Berechtigungen, Einstellungen für die Update-Einschränkung, Zeitplan, Liste der zu installierenden Komponenten, Statistiken, Informationen über gelöschte Workstations; sowie zu Gruppen: Eigenschaften, Konfiguration der Komponenten, Berechtigungen, Einstellungen für die Update-Einschränkung, Zeitplan, Liste der zu installierenden Komponenten, ID der übergeordneten Gruppe.
     Die exportierte Datei kann nachträglich über den Bereich **Datenbankverwaltung** importiert werden.
3. Klicken Sie auf **Exportieren**.
4. Der Pfad des zu speichernden Archivs mit der Datenbank wird entsprechend den Einstellungen des Webbrowsers, in dem das **Verwaltungscenter** geöffnet ist, festgelegt.

Datenbank importieren

Durch den Import einer Datenbank, die Informationen über Objekte eines Antivirus-Netzwerks enthält, können Sie diese Informationen auf einen neuen **Server** oder den **Server**, der bereits im Antivirus-Netzwerks verwendet wird, mit dem Ziel übertragen, Listen gewarteter Workstations beider **Server** zusammenzuführen.

Mit dem **Server**, auf dem der Import erfolgt, können sich alle Workstations verbinden, deren Informationen importiert werden. Stellen Sie vor dem Import sicher, dass Sie genügend Lizenzen für übertragene Workstations haben. Fügen Sie bei Bedarf im Lizenzmanager Lizenzschlüssel vom **Server** hinzu, von dem Informationen über neue Workstations übertragen wurden.

So importieren Sie die Datenbank von einer Datei

1. Klicken Sie auf der Symbolleiste auf **Import**.
2. Geben Sie im nächsten Fenster das ZIP-Archiv mit der Datenbankdatei an. Um die gewünschte Datei auszuwählen, klicken Sie auf .

Importiert werden können nur diejenigen ZIP-Archive, die über die Option **Informationen zu Stationen und Gruppen exportieren** generiert wurden.

3. Klicken Sie auf **Importieren**, um den Import zu starten.
4. Wenn beim Import Workstations und/oder Gruppen mit den IDs, die gleichzeitig in importierten Daten und in der Datenbank des aktuellen **Servers** vorhanden sind, gefunden werden, wird der Bereich **Kollisionen** angezeigt, in dem Sie eine Aktion für duplizierte Objekte auswählen können.

   Listen von Gruppen und Workstations werden in separaten Tabellen angezeigt.

   Wählen Sie für die entsprechende Tabelle von Objekten in der Dropdown-Liste **Importmodus für Stationen** oder **Importmodus für Gruppen** die gewünschte Lösung aus:

   - **Importdaten für alle speichern**. Diese Option gibt an, dass alle Informationen zu duplizierten Objekten in der Datenbank des aktuellen **Servers** durch die Informationen aus der importierten Datenbank ersetzt werden sollen. Die Aktion wird dabei für alle duplizierten Objekte der Tabelle ausgeführt.
   - **Aktuelle Daten für alle speichern**. Diese Option gibt an, dass alle Informationen zu duplizierten Objekten aus der Datenbank des aktuellen **Servers** gespeichert werden sollen. Informationen zu duplizierten Objekten aus der importierten Datenbank werden ignoriert. Die Aktion wird dabei für alle duplizierten Objekte der Tabelle ausgeführt.
   - **Manuell auswählen**. Diese Option ermöglicht, die gewünschte Aktion für jedes duplizierte Objekt manuell festzulegen. Die Liste duplizierter Objekt ist in diesem Modus editierbar. Aktivieren die Optionen neben den Objekten, die gespeichert werden sollen.

   Klicken Sie auf **Speichern**.

Sicherung

Um eine Sicherheitskopie wichtiger Daten des **Servers** zu erstellen, klicken Sie auf der Symbolleiste auf **Sicherheitskopie**. Daten werden in einem GZ-Archiv gespeichert. Dateien, die bei der Sicherung generiert werden, sind identisch mit den Dateien, die beim Start der ausführbaren Datei des **Servers** über den Schalter `backup` erstellt werden.

Dieser Befehl wird im Dokument **Anhänge** unter H3.5. Sicherung kritischer Daten des Dr.Web Servers detailliert beschrieben.

7.9.2. Statistiken des Dr.Web Servers

Über das **Verwaltungscenter** können Sie Statistiken zum **Dr.Web Server** ansehen. Dazu zählen die Ressourcenverwendung des Rechners, auf dem der **Dr.Web Server** installiert ist, und die Netzwerkkommunikation mit den Komponenten des Antivirus-Netzwerks und externen Ressourcen, z. B. mit dem **GUS**.

So lassen Sie Statistiken zum Dr.Web Server anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**.
2. Wählen Sie im nächsten Fenster des Verwaltungsmenüs den Punkt **Dr.Web Server-Statistiken**.
3. Im danach angezeigten Fenster finden Sie die folgenden Statistik-Bereiche:
   - **Client-Aktivitäten**. Hier wird die Anzahl der mit dem **Server** verbundenen Clients angezeigt. Dazu zählen: **Dr.Web Agents**, benachbarte **Dr.Web Server** und Installationsprogramme der **Dr.Web Agents**.
   - **Netzwerkdatenverkehr**. Hier finden Sie Parameter des eingehenden und ausgehenden Datenverkehrs bei der Kommunikation mit dem **Server**.
   - **Nutzung von Systemressourcen**. Hier werden Statistiken zur Systemressourcenverwendung des Rechners, auf dem der **Server** installiert ist, angezeigt.
   - **Microsoft NAP**. Hier finden Sie statistische Daten zum Dr.Web NAP Validator.
   - **Nutzung der Datenbank**. Hier werden Zugriffe auf den **Server** statistisch erfasst.

- **Nutzung von Dateicache**. Hier werden Zugriffe auf den Dateicache des Rechners, auf dem der **Server** installiert ist, statistisch erfasst.
- **DNS-Cache verwenden**. Hier werden Zugriffe auf den Cache, in dem Abfragen an DNS-Server gespeichert werden, statistisch erfasst. Es handelt sich dabei um den Cache des Rechners, auf dem der **Server** installiert ist.
- **Benachrichtigungen**. Hier wird Statistik zum Subsystem der Benachrichtigung des Administrators angezeigt.
- **Repository**. Hier werden Statistiken zum Datenaustausch zwischen dem **Server** und Servern des **GUS** angezeigt.
- **Web-Statistik**. Hier finden Sie Statistik für Zugriffe auf den **Webserver**.
- **Cluster**. Hier werden Zugriffe über das Protokoll statistisch erfasst, mithilfe von dem Server bei der Verwendung eines Clusters von **Servern** in einem Netzwerk mit mehreren Servern synchronisiert werden.

4. Um statistische Daten eines Bereichs anzusehen, klicken Sie auf den Namen des gewünschten Bereichs.
5. In der geöffneten Liste werden die Parameter des Bereichs zusammen mit den dynamischen Zählern angezeigt.
6. Wenn Sie einen statistischen Bereich öffnen, wird gleichzeitig die grafische Darstellung der Änderungen jedes Parameters angezeigt. Achten Sie dabei auf das Folgende:
   - Um die grafische Darstellung zu deaktivieren, klicken Sie auf den Namen des gewünschten Bereichs. Trotz der Deaktivierung der grafischen Darstellung werden die numerischen Werte der Parameter dynamisch aktualisiert.
   - Um die grafische Darstellung erneut zu aktivieren, klicken Sie wieder auf den Namen des gewünschten Bereichs.
   - Namen der Bereiche und ihrer Parameter, für welche die grafische Darstellung aktiviert ist, werden fett markiert.
7. Um die Aktualisierungshäufigkeit zu ändern, verwenden Sie eine der folgenden Möglichkeiten:
   - Wählen Sie in der Dropdown-Liste **Aktualisierungsrate** die gewünschte Aktualisierungshäufigkeit. Die neue Aktualisierungshäufigkeit der numerischen und grafischen Daten wird automatisch übernommen.
   - Klicken Sie auf **Aktualisieren**, um alle statistischen Daten gleichzeitig zu aktualisieren.
8. Wenn Sie mit dem Mauszeiger auf eine grafische Darstellung zeigen, wird der entsprechende numerische Werte wie folgt angezeigt:
   - **Abs** ist der absolute Wert des Parameters.
   - **Delta** ist die Änderung des Werts vom Parameter relativ seinem vorherigen Wert gemäß der aktuellen Aktualisierungshäufigkeit.
9. Um die Parameter eines Bereichs auszublenden, klicken Sie auf das Pfeilsymbol links vom Namen des Bereichs. Beim Ausblenden der Parameter des Bereichs werden die grafischen Daten gelöscht. Beim erneuten Einblenden werden sie wieder gezeichnet.

7.9.3. Sicherungskopien

Der Bereich **Sicherungskopien** ermöglicht Ihnen, Sicherungskopien wichtiger Daten des **Servers** auf Verzeichnis- und Dateiebene anzuzeigen und bei Bedarf lokal zu speichern.

Folgende Objekte werden bei einer Sicherung gespeichert: Einstellungen des Repository, Konfigurationsdateien, Schlüssel, Zertifikate, Sicherungskopie der eingebetteten Datenbank.

Sicherungskopien wichtiger Daten des **Servers** werden im folgenden Fällen gespeichert:

- Bei der Ausführung des Aufgabe **Sicherung der kritischen Daten des Servers** entsprechend dem Zeitplan des **Servers**.

- Beim Start der ausführbaren Datei des **Servers** über den Befehl mit dem Schalter `backup`. Dieser Befehl wird im Dokument **Anhänge** im H3.5. Sicherung kritischer Daten des Dr.Web Servers detailliert beschrieben.

Informationen zu Sicherungskopien anzeigen

Um Informationen zu einer Sicherungskopie anzuzeigen, wählen Sie in der baumartigen Struktur von Sicherungskopien das gewünschte Objekt aus. Das Eigenschaftenpanel mit Informationen zum Objekt wird angezeigt: **Typ**, **Größe** (nur für einzelne Dateien), **Erstellungsdatum** und **Änderungsdatum**.

Sicherungskopien verwalten

Verwenden Sie zur Verwaltung von Sicherungskopien die folgenden Schaltflächen auf der Symbolleiste:

Exportieren. Diese Option gibt an, dass die Sicherungskopie des ausgewählten Objektes auf dem Rechner, auf dem das **Verwaltungscenter** geöffnet ist, gespeichert werden soll.

Ausgewählte Objekte entfernen. Diese Option gibt an, dass die in der Baumstruktur gewählten Objekte endgültig gelöscht werden sollen.

Sicherungskopie exportieren

So speichern Sie eine Sicherungskopie auf Ihrem Rechner

1. Wählen Sie in der baumförmigen Struktur die gewünschten Sicherungskopien oder einzelne Dateien der Sicherungskopien aus. Um die ganze Sicherungskopie auszuwählen, wählen Sie in der Struktur das Verzeichnis, das dieser Sicherungskopie entspricht. Um mehrere Objekte auf einmal auszuwählen, verwenden Sie die STRG- oder UMSCHALTTASTE.

   Achten Sie beim Export auf die Typen der zu exportierenden Objekte:

   a) ZIP-Archive von Sicherungskopien werden bei der Auswahl folgender Objekte generiert:
      - Ganze Sicherungskopien (bei der Auswahl der Verzeichnisse, die den Sicherungskopien entsprechen).
      - Einige einzelne Dateien in Sicherungskopien.

   b) Einzelne Dateien in Sicherungskopien. Wenn Sie nur eine Datei zum Import ausgewählt haben, wird diese im Originalformat gespeichert.
2. Klicken Sie auf der Symbolleiste auf **Exportieren**.
3. Der Pfad der zu speichernden Objekte wird entsprechend den Einstellungen des Webbrowsers, in dem das **Verwaltungscenter** geöffnet ist, festgelegt.

7.10. Besonderheiten eines Netzwerks mit mehreren Dr.Web Servern

Dr.Web Enterprise Security Suite ermöglicht Ihnen, ein Antivirus-Netzwerk mit mehreren **Dr.Web Servern** aufzubauen. In diesem Multi-Server-Netzwerk wird jede Workstation einem bestimmten **Server** zugewiesen. Dadurch kann die Last gleichmäßig verteilt werden.

Einzelne **Server** können über eine hierarchische Struktur miteinander verbunden werden. Diese Topologie ermöglicht eine gleichmäßige Verteilung der Lasten zwischen **Servern**.

Damit **Server** miteinander kommunizieren können, wird das spezielle *Protokoll für die Server-zu-Server-Synchronisierung* eingesetzt.

Das Protokoll für die Server-zu-Server-Synchronisierung bietet die folgenden Vorteile:

- Verteilung von Updates an **Server** innerhalb des Antivirus-Netzwerks.
- Schnelle Übertragung von über das **Dr.Web GUS** heruntergeladenen Updates.
- Übertragung von Statistiken zu geschützten Workstations zwischen **Servern**.
- Übertragung von Lizenzen für geschützte Workstations zwischen **Servern**.

7.10.1. Aufbau eines Netzwerks mit mehreren Dr.Web Servern

In einem Antivirus-Netzwerk kann mehrere **Dr.Web Server** eingerichtet werden. Jeder **Dr.Web Agent** stellt eine Verbindung mit einem der **Server** her. Ein **Server** und mit ihm verbundene Workstations bilden ein separates Antivirus-Netzwerk, wie es in vorherigen Kapiteln beschrieben wurde.

Dr.Web Enterprise Security Suite bietet die Möglichkeit, solche Antivirus-Netzwerke miteinander zu verbinden. Dies wird ermöglicht durch die Kommunikation zwischen den **Dr.Web Servern**.

Dr.Web Server sendet an einen anderen Dr.Web Server:

- Updates für die Software und Virendatenbanken. Dabei kann nur einer von ihnen die über das **Dr.Web GUS** heruntergeladenen Updates erhalten.
- Informationen zu erkannten Bedrohungen, Statistiken usw.
- Lizenzen für geschützte Workstations (die Verteilung von Lizenzen an **Server** wird im Lizenz-Manager konfiguriert).

Dr.Web Enterprise Security Suite bietet zwei Möglichkeiten für den Informationsaustausch zwischen Dr.Web Servern:

- *Verbindungen des Typs Übergeordnet-Untergeordnet*. Bei diesem Modell übermittelt der übergeordnete Server Updates an untergeordnete Server und erhält Informationen zu Ereignissen zurück.
- *Peer-zu-Peer*-Verbindungen. Bei diesem Modell werden die Übertragungsrichtung und Informationstypen individuell festgelegt.

In der Abbildung 7-1 finden Sie den exemplarischen Aufbau eines Netzwerks mit mehreren **Servern**.

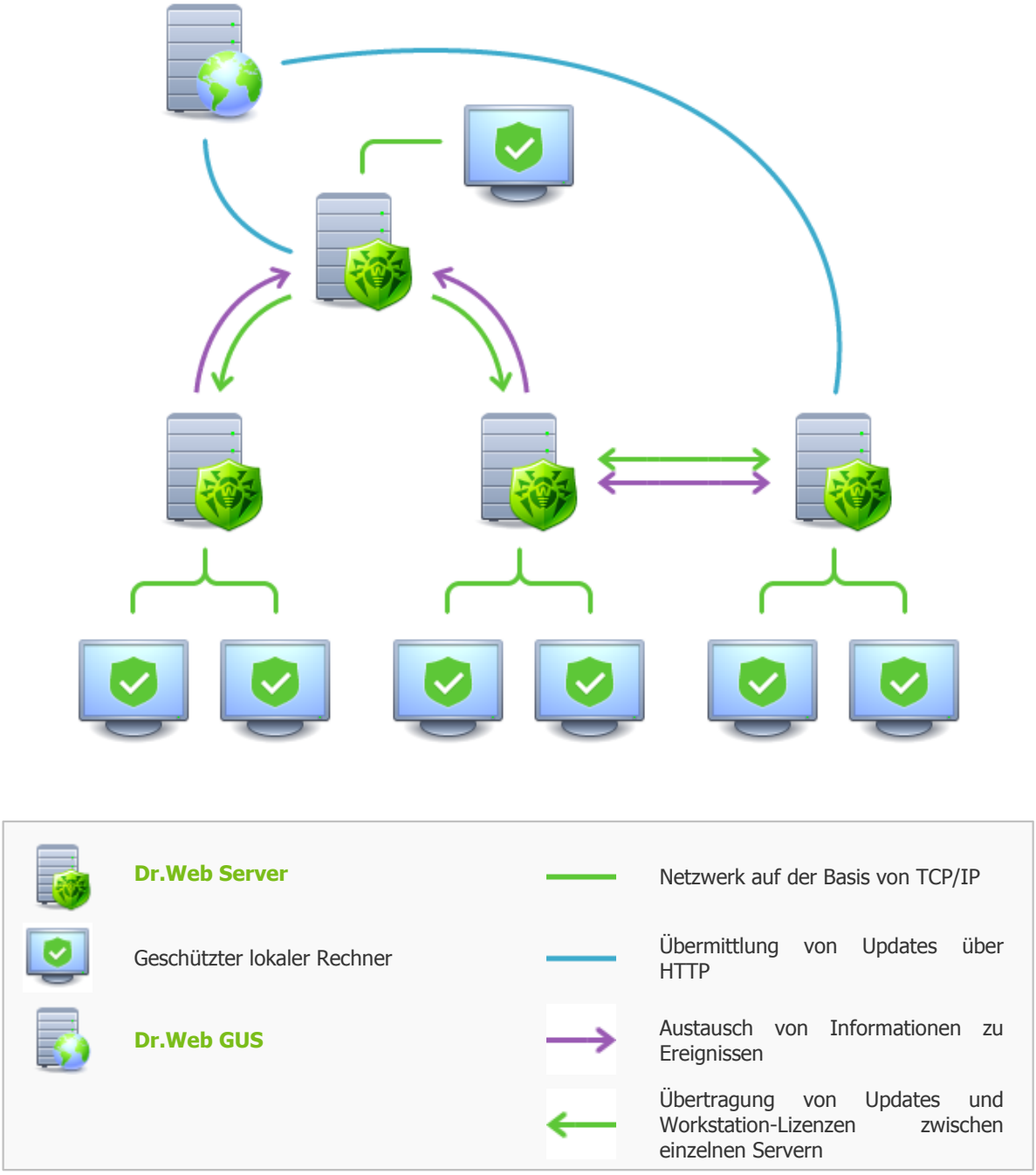

Dr.Web Server
Geschützter lokaler Rechner
Dr.Web GUS
Netzwerk auf der Basis von TCP/IP
Übermittlung von Updates über HTTP
Austausch von Informationen zu Ereignissen
Übertragung von Updates und Workstation-Lizenzen zwischen einzelnen Servern

Abbildung 7-1: Netzwerk mit mehreren Servern

Einige Vorteile des Antivirus-Netzwerks mit mehreren Dr.Web Servern:

1. Updates von Servern des **Dr.Web GUS** können über einen **Dr.Web Server** heruntergeladen werden und dann an weitere **Server** direkt oder indirekt verteilt werden.

Server, die Updates vom übergeordneten **Server** beziehen, erhalten keine Updates über das **GUS**, selbst wenn die einsprechende Aufgabe geplant wurde.

Da der übergeordnete **Server** eventuell vorübergehend nicht verfügbar sein kann, empfiehlt es sich, im Zeitplan des untergeordneten **Servers** eine Aufgabe zum Update über das **GUS** zu planen. Dadurch können die **Agents**, die mit dem untergeordneten **Server** verbunden sind, aktualisierte Virendatenbank und Programmmodule erhalten (s. dazu auch Allgemeine Konfiguration des Repository).

In der Aufgabe zum Update über das **GUS**, die auf dem übergeordneten **Server** geplant wird, müssen Sie angeben, dass Updates für die Server-Software aller Betriebssysteme, unter denen untergeordnete **Server** laufen, erhalten werden sollen (mehr dazu finden Sie unter Allgemeine Konfiguration des Repository).

2. Workstations können auf mehrere **Server** verteilt werden. Dies reduziert die Arbeitslast auf jedem **Server**.
3. Die vom mehreren **Servern** gesendeten Informationen können auf einem gesammelt werden. Diese zusammengefassten Informationen könne dann über das **Verwaltungscenter** auf diesem **Server** angezeigt werden.

Dr.Web Enterprise Security Suite überwacht und unterbindet eventuelle zyklische Datenflüsse.

4. Verfügbare Lizenzen können an einen benachbarten **Server** übertragen werden. Der Lizenzschlüssel bleibt dabei auf dem verteilenden **Server**: Verfügbare Lizenzen werden an einen benachbarten **Server** für einen bestimmten Zeitraum übertragen. Nach dessen Ablauf werden sie widerrufen.

7.10.2. Verbindungen zwischen Dr.Web Servern konfigurieren

Um ein Netzwerk mit mehreren **Servern** aufzubauen, müssen Sie eine Kommunikation zwischen ihnen konfigurieren.

Es empfiehlt sich, die Struktur des Antivirus-Netzwerks im Voraus sorgfältig zu planen. Im Topologiediagramm müssen alle eventuellen Datenflüsse und Beziehungen zwischen involvierten Elementen deutlich angezeigt werden. Konfigurieren Sie dann alle Verbindungen mit benachbarten **Servern** für jeden **Server** innerhalb des Netzwerks. Zwei oder mehr **Server** gelten als benachbart, wenn mindestens ein Datenfluss zwischen ihnen besteht.

Beispiel für die Konfiguration der Kommunikation zwischen übergeordneten und untergeordneten Dr.Web Servern

Die mit Sternchen * gekennzeichneten Felder sind Pflichtfelder.

1. Stellen Sie sicher, dass beide **Dr.Web Server** voll funktionsfähig sind.
2. Geben Sie für jeden **Dr.Web Server** einen erkennbaren und leicht zu merkenden Namen an. Dadurch vermeiden Sie eventuelle Fehler bei der Konfiguration der Kommunikation zwischen den **Dr.Web Servern** und bei ihrer Verwaltung. Wechseln Sie dafür zu **Verwaltungscenter** **Administrierung** → **Dr.Web Server-Konfiguration** und geben Sie auf der Registerkarte **Allgemein** im Feld **Name** den gewünschten Namen an. In unserem Beispiel hat der übergeordnete **Server** den Namen `MAIN`, und der untergeordnete – `AUXILIARY`.
3. Aktiveren Sie für beide **Dr.Web Server** das Serverprotokoll. Wechseln Sie dafür zum Menü des **Verwaltungscenters** **Administrierung** → **D.Web Server-Konfiguration** und aktivieren Sie auf der Registerkarte **Module** das Kontrollkästchen **Protokoll von Dr.Web Server** (mehr dazu finden Sie unter Module).

Wenn das Serverprotokoll nicht aktiviert ist, werden Sie bei der Einrichtung einer neuen Verbindung im **Verwaltungscenter** aufgefordert, dieses zu aktivieren. Dabei wird der Link zum entsprechenden Bereich des **Verwaltungscenters** angezeigt.

4. Starten Sie beide **Dr.Web Server** neu.
5. Fügen Sie über das **Verwaltungscenter** des untergeordneten **Servers** (AUXILIARY) den übergeordneten **Server** (MAIN) zur Liste benachbarter **Server**. Wählen Sie dafür im Hauptmenü den Punkt **Nachbar**. Das Fenster mit der hierarchischen Liste der **Server** des Antivirus-Netzwerks, die diesem **Server** benachbart sind, wird geöffnet. Um den **Server** zur Liste hinzuzufügen, klicken Sie auf der Symbolleiste auf **Verbindung herstellen**.

   Das Fenster mit der Beschreibung der Beziehung zwischen dem aktuellen und hinzuzufügenden **Server** wird geöffnet. Legen Sie hier die folgenden Einstellungen fest:

   - **Typ** der zu erstellenden Verbindung – **Übergeordnet**.
   - **Name**. Hier wird der Name des übergeordneten **Servers** (MAIN) angegeben.
   - **Passwort***. Hier wird ein beliebiges Passwort für den Zugriff auf den übergeordneten **Server** angegeben.
   - **Eigene Schlüssel des Dr.Web Servers**. Hier wird die Liste der öffentlichen Schlüssel des einzustellenden **Servers** angezeigt. Klicken Sie auf und wählen Sie den Schlüssel drwcsd.pub des aktuellen **Servers** aus. Um einen weiteren Schlüssel hinzuzufügen, klicken Sie auf und geben Sie im neuen Feld den gewünschten Schlüssel an.
   - **Schlüssel des benachbarten Dr.Web Servers***. Hier wird die Liste der öffentlichen Schlüssel des zu verbindenden übergeordneten **Servers** angezeigt. Klicken Sie auf und wählen Sie den Schlüssel drwcsd.pub des übergeordneten **Servers** aus. Um einen weiteren Schlüssel hinzuzufügen, klicken Sie auf und geben Sie im neuen Feld den gewünschten Schlüssel an.
   - **Adresse***. Hier wird die Netzwerkadresse des übergeordneten **Servers** und der Port für die Verbindung angegeben. Der Wert dieser Option muss im Format *<Serveradresse>:<Port>* angegeben werden.

   Sie können nach im Netzwerk verfügbaren **Servern** durchsuchen. Gehen Sie dafür so vor:

   a) Klicken Sie auf den Pfeil rechts vom Feld **Adresse**.
   b) Geben Sie im geöffneten Fenster Netzwerke an. Dafür können Sie die folgenden Eingabeformate verwenden: Durch einen Bindestrich getrennt (z. B. 10.4.0.1-10.4.0.10), durch ein Komma und Leerzeichen getrennt (z. B. 10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90), Durch Angabe eines Netzwerkpräfixes (z. B.10.4.0.0/24).
   c) Klicken Sie auf . Das Netzwerk wird nach verfügbaren **Servern** durchsucht.
   d) Wählen Sie aus der Liste der verfügbaren **Server** einen **Server** aus. Ihre Adresse wird im Feld **Adresse** angezeigt.

   - **Adresse des Dr.Web-Sicherheitscenters**. Hier können Sie die Adresse der Startseite des **Verwaltungscenters** vom übergeordneten **Server** angeben (weitere Informationen finden Sie unter Dr.Web Sicherheitscenter).
   - In der Dropdown-Liste **Verbindungsparameter** wird festgelegt, wie sich die **Server** miteinander verbinden sollen.
   - Legen Sie in den Dropdown-Listen **Verschlüsselung** und **Komprimierung** die Einstellungen für die Verschlüsselung und Komprimierung des Datenverkehrs zwischen den involvierten **Servern** (mehr dazu finden Sie unter Datenverkehr verschlüsseln und komprimieren).
   - **Laufzeit vergebener Lizenzen**. Hier wird der Zeitraum angegeben, für den Lizenzen aus dem Schlüssel des übergeordneten **Servers** verteilt werden sollen. Diese Option wird verwendet, wenn der übergeordnete **Server** Lizenzen an den aktuellen **Server** verteilen soll.
   - **Zeitraum für Verlängerung von erhaltenen Lizenzen**. Diese Option wird bei der Herstellung einer Verbindung mit einem übergeordneten **Server** nicht verwendet.

- **Synchronisationszeitraum der Lizenzen**. Hier wird das Zeitintervall angegeben, mit dem Informationen zu vergebenen Lizenzen zwischen den **Servern** synchronisiert werden sollen.
- Die Optionen in den Bereichen **Lizenzen**, **Updates** und **Ereignisse** sind für die Verbindungen des Typs *übergeordnet-untergeordnet* bereits eingestellt und können nicht geändert werden:
  - Der übergeordnete **Server** überträgt Lizenzen an untergeordnete **Server**.
  - Der übergeordnete **Server** überträgt Updates an untergeordnete **Server**.
  - Der übergeordnete **Server** erhält von untergeordneten **Servern** Informationen zu Ereignissen.
- Im Bereich **Update-Restriktionen** > **Ereignisse** können Sie einen Zeitplan für die Übertragung der Ereignisse vom aktuellen **Server** auf den übergeordneten konfigurieren (der Modus für die Übertragung von Ereignissen kann ebenso wieder Aktualisierungsmodus im Bereich Updates für Workstations einschränken geändert werden).

Klicken Sie auf **Speichern**.

Der übergeordnete **Server** (`MAIN`) wird abschließend in die Ordner **Primär** und **Offline** aufgenommen (s. die Abb. 7-2).

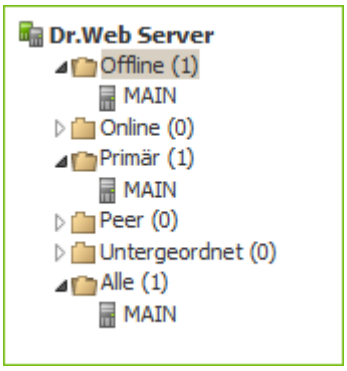


Abbildung 7-2.

6. Fügen Sie über das **Verwaltungscenter** des übergeordneten **Servers** (`MAIL`) den untergeordneten **Server** (`AUXILIARY`) zur Liste benachbarter **Server**. Wählen Sie dafür im Hauptmenü den Punkt **Nachbar**. Das Fenster mit der hierarchischen Liste der **Server** des Antivirus-Netzwerks, die diesem benachbart sind, wird geöffnet. Um den **Server** zur Liste hinzuzufügen, klicken Sie auf der Symbolleiste auf **Verbindung herstellen**.

   Das Fenster mit der Beschreibung der Beziehung zwischen dem aktuellen und hinzuzufügenden **Server** wird geöffnet. Legen Sie hier die folgenden Einstellungen fest:

   - **Typ** der zu erstellenden Verbindung – **Untergeordnet**.
   - **Name**. Hier wird der Name des untergeordneten **Servers** (`AUXILIARY`) angegeben.
   - **Passwort***. Geben Sie hier das Passwort an, das Sie im Schritt **5** festgelegt haben.
   - **Eigene Schlüssel des Dr.Web Servers**. Hier wird die Liste der öffentlichen Schlüssel des einzustellenden **Servers** angezeigt. Klicken Sie auf und wählen Sie den Schlüssel `drwcsd.pub` des aktuellen **Servers** aus. Um einen weiteren Schlüssel hinzuzufügen, klicken Sie auf und geben Sie im neuen Feld den gewünschten Schlüssel an.
   - **Schlüssel des benachbarten Dr.Web Servers***. Hier wird die Liste der öffentlichen Schlüsseln des zu verbindenden untergeordneten **Servers** angezeigt. Klicken Sie auf und wählen Sie den Schlüssel `drwcsd.pub` des untergeordneten **Servers**. Um einen weiteren Schlüssel hinzuzufügen, klicken Sie auf und geben Sie im neuen Feld den gewünschten Schlüssel an.
   - **Adresse des Dr.Web-Sicherheitscenters**. Hier können Sie die Adresse der Startseite des **Verwaltungscenters** vom untergeordneten **Server** angeben (weitere Informationen finden Sie unter Dr.Web Sicherheitscenter).

- In der Dropdown-Liste **Verbindungsparameter** wird festgelegt, wie sich die **Server** miteinander verbinden sollen.
- Legen Sie in den Dropdown-Listen **Verschlüsselung** und **Komprimierung** die Einstellungen für die Verschlüsselung und Komprimierung des Datenverkehrs zwischen den involvierten **Servern** (mehr dazu finden Sie unter Datenverkehr verschlüsseln und komprimieren).
- **Laufzeit vergebener Lizenzen**. Diese Option wird bei der Herstellung einer Verbindung mit einem untergeordneten **Server** nicht verwendet.
- **Zeitraum für Verlängerung von erhaltenen Lizenzen**. Hier wird der Zeitraum bis zum Ablauf der Lizenz angegeben, ab dem der untergeordnete **Server** die Verlängerung der von dem aktuellen **Server** erhaltenen Lizenz initiiert. Diese Option wird verwendet, wenn der untergeordnete **Server** Lizenzen vom aktuellen **Server** verteilt bekommen soll.
- **Synchronisationszeitraum der Lizenzen**. Hier wird das Zeitintervall angegeben, mit dem Informationen zu vergebenen Lizenzen zwischen den **Servern** synchronisiert werden sollen.
- Die Optionen in den Bereichen **Lizenzen**, **Updates** und **Ereignisse** sind für die Verbindungen des Typs *übergeordnet-untergeordnet* bereits eingestellt und können nicht geändert werden:
  - Der untergeordnete **Server** erhält vom übergeordneten **Server** Lizenzen.
  - Der untergeordnete **Server** erhält vom übergeordneten **Server** Updates.
  - Der untergeordnete **Server** sendet an den übergeordneten **Server** Informationen zu Ereignissen.
- Im Bereich **Update-Restriktionen** > **Updates** können Sie einen Zeitplan für die Übertragung der Updates vom aktuellen **Server** auf den untergeordneten konfigurieren (der Modus für die Übertragung von Updates kann ebenso wieder Aktualisierungsmodus im Bereich Updates für Workstations einschränken geändert werden).

Klicken Sie auf **Speichern**.

Der untergeordnete **Server** (`AUXILIARY`) wird abschließend in die Ordner **Untergeordnet** und **Offline** aufgenommen (s. die Abb. 7-3).

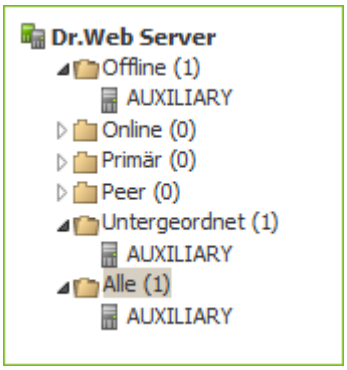


Abbildung 7-3.

7. Warten Sie, bis die **Server** miteinander verbunden sind. Der Vorgang dauert normalerweise etwa eine Minute. Um die Liste von **Servern** zu aktualisieren, drücken Sie die Taste F5. Sobald eine Verbindung hergestellt ist, wird der untergeordnete **Server** (`AUXILIARY`) vom Ordner **Offline** in den Ordner **Online** verschoben (s. die Abb. 7-4).

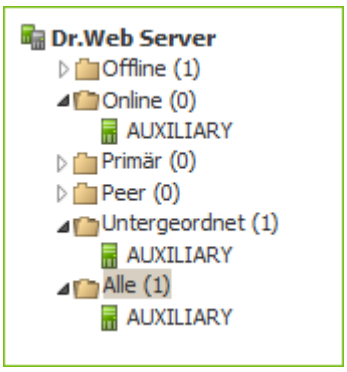


Abbildung 7-4.

8. Öffnen Sie das **Verwaltungscenter** des untergeordneten **Servers** (`AUXILIARY`) und stellen Sie sicher, dass der übergeordnete **Server** (`MAIN`) mit dem untergeordneten (`AUXILIARY`) verbunden ist (s. die Abb. 7-5).

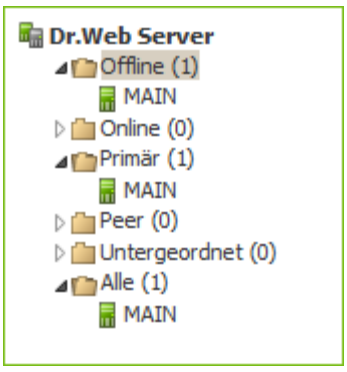


Abbildung 7-5.

Mehrere **Server**, für die das gleiche Password und den gleichen öffentlichen Schlüssel `drwcsd.pub` angegeben wurden, lassen sich miteinander nicht verbinden.

Es empfiehlt sich, bei der Einstellung von Peer-to-Peer-Verbindungen zwischen **Servern** die Adresse des zu verbindenden **Servers** nur in den Einstellungen eines von ihnen anzugeben.

Das hat keine Auswirkungen auf die Kommunikation zwischen den **Servern**. Dadurch vermeiden Sie aber eventuelle Einträge `Link with the same key id is already activated` im Protokoll der **Server**.

In folgenden Fällen kann die Verbindung zwischen Dr.Web Servern nicht hergestellt werden:

- Netzwerkprobleme.
- Eine falsche Adresse des übergeordneten **Servers** wurde beim Konfigurieren der Verbindung angegeben.
- Ungültige öffentliche Schlüssel `drwcsd.pub` wurden auf einem der **Server** angegeben.
- Ein falsches Passwort wurde auf einem der **Server** angegeben (Passwörter für die zu verbindenden **Server** stimmen nicht überein).

7.10.3. Antivirus-Netzwerk mit mehreren Dr.Web Servern

Das Besondere am Netzwerk mit mehreren **Servern** ist, dass nur einige **Dr.Web Server** (i.d.R. einer der übergeordneten **Server**) Updates über das **Dr.Web GUS** beziehen können. Dabei muss die

Aufgabe zur Aktualisierung nur auf diesen **Servern** konfiguriert werden (mehr dazu finden Sie unter Zeitplan des Dr.Web Servers konfigurieren). Ein beliebiger **Server**, der Updates über das **Dr.Web GUS** oder von einem anderen **Server** erhalten hat, verteilt sie sofort auf alle mit ihm verbundenen untergeordneten **Server** und diejenigen Peer-Server, für die diese Option aktiviert wurde.

> **Dr.Web Enterprise Security Suite** unterbindet automatisch, dass ein bereits erhaltenes Update aufgrund einer fehlerhaft aufgebauten Netzwerktopologie oder falschen Konfiguration der **Server** erneut an den gleichen **Server** übertragen wird.

Der Administrator kann auch Übersichtsinformationen zu den wichtigsten Ereignissen auf den Workstations, die mit einem **Server** über die Server-zu-Server-Kommunikation verbunden sind, anzeigen lassen. Bei der oben beschriebenen Konfiguration werden diese Informationen auf dem übergeordneten **Server** gesammelt.

So lassen Sie Informationen zu Ereignissen auf allen mit dem aktuellem Dr.Web Server verbundenen Dr.Web Servern anzeigen

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Nachbar**.
2. Wählen Sie im nächsten Fenster im Bereich **Tabellen** des Verwaltungsmenüs den Punkt **Gesamtreport**, um Informationen zur Gesamtzahl der Einträge über die Ereignisse auf den benachbarten **Servern** anzuzeigen. In der Tabelle mit der Statistik zu den benachbarten **Servern** werden die folgenden Daten angezeigt:
   - **Infektionen**. Hier werden alle Infektionen angezeigt, die auf den mit den benachbarten **Servern** verbundenen Workstations erkannt wurden.
   - **Fehler**. Hier werden alle Scan-Fehler angezeigt.
   - **Statistik**. Hier werden alle erkannten Infektionen statistisch erfasst.
   - **Start/Beenden**. Hier werden Information zum Start und Beenden von Scan-Aufgaben angezeigt.
   - **Status**. Hier wird der Zustand der auf den Workstations installierten Antivirensoftware angezeigt.
   - **Alle Netzwerkinstallationen**. Hier werden Netzwerkinstallationen der **Agents** angezeigt.
3. Um auf die Seite mit tabellarisch dargestellten Detailinformationen über Ereignisse auf den benachbarten **Servern** zu gelangen, klicken Sie in der Tabelle des Bereiches **Gesamtdaten** auf die Ziffer, die für die Anzahl der Einträge über das benötigte Ereignis steht.
4. Alternativ können Sie im Verwaltungsmenü den entsprechenden Punkt (s. den Schritt 2) des Bereichs **Tabellen** wählen, um tabellarisch dargestellte Informationen über die Ereignisse auf den benachbarten **Servern** anzuzeigen.
5. Um Daten für einen bestimmten Zeitraum anzeigen zu lassen, wählen Sie in der Dropdown-Liste den anzuzeigenden Zeitraum relativ zum jeweils aktuellen Tag an, oder geben Sie auf der Symbolleiste einen beliebigen Zeitraum an. Im letzten Fall müssen Sie die gewünschten Datumsangaben manuell eingeben oder auf das Kalendersymbol neben den Datumsfeldern klicken. Klicken Sie zur Anzeige der Daten auf **Aktualisieren**.
6. Um die Tabelle auszudrucken oder später zu bearbeiten, klicken Sie auf der Symbolleiste eine der folgenden Schaltflächen an:

   Daten in der CSV-Datei speichern.

   Daten in der HTML-Datei speichern.

   Daten in der XML-Datei speichern.

   Daten in der PDF-Datei speichern.

7.10.4. Mehrere Dr.Web Server mit einer gemeinsamen Datenbank verknüpfen

Um eine gemeinsame Datenbank verwenden zu können, müssen alle **Dr.Web Server** von der gleichen Version sein.

Server innerhalb des Clusters sollten mithilfe ihrer Installationspakete aktualisiert werden. Alle **Server** müssen angehalten werden und der Reihe nach aktualisiert werden. Sie sollten auf die Aktualisierung über das **Verwaltungscenter** (Aktualisierung auf eine neuere Revision) verzichten, da bei der Verwendung einer gemeinsamen Datenbank können nach der Aktualisierung des ersten **Servers** alle restlichen **Server** nicht mehr betrieben und aktualisiert werden.

Damit Sie ein Antivirus-Netzwerk mit mehreren **Dr.Web Servern** und einer Datenbank einrichten können, müssen folgende Bedingungen erfüllt sein:

1. Alle **Server** müssen die gleichen Schlüssel `drwcsd.pub`, `drwcsd.pri`, Zertifikate `certificate.pem`, `private-key.pem` und den gleichen Schlüssel `agent.key` haben.
2. In der Konfigurationsdatei des **Verwaltungscenters** `webmin.conf` muss in der Einstellung `ServerName` für alle **Server** der gleiche DNS-Name des **Servers** festgelegt werden.
3. Auf dem DNS-Server des Netzwerks muss der gemeinsame Clustername für jeden einzelnen **Server** registriert werden sowie eine Lastenausgleichsmethode festgelegt werden.
4. In den Konfigurationsdateien der **Server** `drwcsd.conf` muss für alle **Server** die gleiche externe Datenbank festgelegt werden.
5. Im Server-Zeitplan dürfen die Aufgaben **Purge Old Data**, **Prepare and send fiscal report periodic job**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge unsent IS events** nur auf einem der **Server** (auf dem leistungsfähigsten, falls sie nicht identisch sind) geplant werden.

Kapitel 8: Komponenten von Dr.Web Enterprise Security Suite aktualisieren

Bevor Sie mit der Aktualisierung der **Dr.Web Enterprise Security Suite** und ihrer einzelnen Komponenten anfangen, sollten Sie sicherstellen, dass Sie über eine aktive Internetverbindung verfügen und das TCP/IP-Protokoll richtig konfiguriert haben. Überprüfen Sie vor allem, dass der DNS-Dienst aktiviert und richtig konfiguriert ist.

Die Software und Virendatenbanken können sowohl manuell als auch nach vorgegebenem Zeitplan des **Servers** und **Agents** aktualisiert werden.

Bevor Sie mit der Aktualisierung der Software beginnen, sollten Sie das Repository, insbesondere den Zugriff auf das **Dr.Web GUS** (s. Allgemeine Konfiguration des Repository), entsprechend konfigurieren.

8.1. Dr.Web Server aktualisieren und aus einer Sicherungskopie wiederherstellen

Das **Verwaltungscenter** bietet Ihnen die folgenden Möglichkeiten für die Verwaltung der Software des **Dr.Web Servers**:

- Aktualisierung der Software des **Servers** auf eine der verfügbaren Versionen, die über das **GUS** heruntergeladen und im Repository des **Servers** gespeichert wurden. Eine detaillierte Beschreibung der Einstellungen für die Aktualisierung des Repository über das **GUS** finden Sie im Abschnitt Dr.Web Server-Repository verwalten.
- Zurücksetzung der Software des **Servers** auf eine gespeicherte Sicherungskopie. Sicherungskopien des **Servers** werden bei der Aktualisierung auf eine neuere Version im Bereich **Dr.Web Server-Updates** automatisch erstellt (s. den Schritt 4 unten).

Der **Server** kann innerhalb der Version **10** mithilfe der Distribution des **Servers** aktualisiert werden. Hinweise zu diesem Update finden Sie in der **Installationsanleitung** unter Dr.Web Server unter Windows® aktualisieren oder Dr.Web Server unter Betriebssystemen der UNIX®-Familie aktualisieren.

Einige Updates des **Servers** innerhalb der Versionsnummer **10** enthalten keine Distributionsdatei. Aus diesem Grund können einige von ihnen nur über das **Verwaltungscenter** installiert werden.

Wenn der **Server** unter UNIX-basierten Betriebssystemen über das **Verwaltungscenter** aktualisiert wird, bleibt die Version des **Servers** im Package Manager unverändert.

So verwalten Sie die Software des Dr.Web Servers

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Dr.Web Server**.
2. Um zur Liste der Versionen des **Servers** zu wechseln, führen Sie eine der folgenden Aktionen durch:
   - Klicken Sie im Hauptfenster auf die aktuelle Version des **Servers**.
   - Klicken Sie die Schaltfläche **Liste der Versionen** an.
3. Der Bereich **Dr.Web Server-Updates** mit der Liste verfügbarer Updates und Sicherungskopien des **Servers** wird geöffnet.

- In der Liste **Aktuelle Version** wird die zum aktuellen Zeitpunkt verwendete Version des **Servers** angezeigt. Unter **Änderungsliste** werden neue Features und behobene Probleme aufgeführt.
- In der Liste **Alle Versionen** werden die Updates des **Servers**, die über das **GUS** heruntergeladen wurden, aufgelistet. Im Bereich **Änderungsliste** werden behobene Fehler und neue Features, die jedes der Updates mitbringt, kurz beschrieben.

Für die Version, die bei der Erstinstallation des **Servers** verwendet wurde, ist der Bereich **Änderungsliste** leer.

- In der Liste **Sicherungskopien** werden alle Sicherungskopien des **Servers** aufgelistet. Im Bereich **Beschreibung** finden Sie das Datum der jeweiligen Sicherung.

4. Um die Software des **Servers** zu aktualisieren, aktivieren Sie in der Liste **Alle Versionen** die Option neben der gewünschten Version des **Servers** und klicken Sie auf **Speichern**.

Bei der Aktualisierung handelt es sich um eine Upgrade des **Servers** auf eine neuere Version: Ein Downgrade ist nicht möglich.

Bei der Aktualisierung des **Servers** wird als Sicherungskopie die aktuelle Version gespeichert (sie wird in den Bereich **Sicherungskopien** verschoben), und die Version, auf die aktualisiert wird, wird vom Bereich **Alle Versionen** in den Bereich **Aktuelle Version** verschoben.

Sicherungskopien werden im folgenden Verzeichnis abgespeichert:

`var` → `update_backup_`*<alte_Version>*`_`*<neue_Version>*.

Bei der Aktualisierung wird das Protokoll `var` → `dwupdater.log` erstellt und erweitert.

5. Um die Software des **Servers** aus einer gespeicherten Sicherungskopie wiederherzustellen, aktivieren Sie in der Liste **Sicherungskopien** die Option neben der gewünschten Version des **Servers** und klicken Sie auf **Speichern**.

Beim Rollback des **Servers** wird die wiederherzustellende Sicherungskopie in den Bereich **Aktuelle Version** verschoben.

8.2. Komponenten von Dr.Web Enterprise Security Suite manuell aktualisieren

Das GUS auf Updates überprüfen

So überprüfen Sie die Verfügbarkeit neuer Updates für Produkte von Dr.Web Enterprise Security Suite

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Status des Repository**.
2. Im geöffneten Fenster werden Informationen zu allen Komponenten, das Datum ihrer letzten Revision und ihr aktueller Status angezeigt. Um die Verfügbarkeit neuer Updates auf dem Server des **GUS** zu überprüfen, klicken Sie auf **Auf Updates überprüfen.**
3. Wenn eine zu überprüfende Komponente nicht mehr aktuell ist, wird sie beim Überprüfen automatisch aktualisiert. Die Aktualisierung erfolgt anhand der Einstellungen des Repository (weitere Informationen finden Sie unter Dr.Web Server-Repository verwalten).

Software einer Workstation aktualisieren

So aktualisieren Sie die Software einer Workstation

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Antivirus-Netzwerk**. Klicken Sie in der hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe.
2. Klicken Sie auf der Symbolleiste auf **Komponentenverwaltung**. Wählen Sie im nächsten Untermenü einen der folgenden Punkte:
   - **Fehlkomponenten aktualisieren** erzwingt die Zurücksetzung des Fehlerstatus und Aktualisierung der Komponenten, die zuletzt nicht aktualisiert werden konnten.
   - **Alle Komponenten aktualisieren** erzwingt die Aktualisierung aller Komponenten, darunter erfolgreich aktualisierter Komponenten.

Bei einer erzwungenen Aktualisierung aller Komponenten ist ein Neustart der Workstation erforderlich. Folgen Sie dann den Anweisungen des **Agents**.

8.3. Geplante Aktualisierungen

Sie können einen Zeitplan auf einem bestimmten **Server** so konfigurieren, dass die Software regelmäßig aktualisiert wird (mehr zum Aufgabenzeitplan finden Sie unter Zeitplan des Dr.Web Servers konfigurieren).

So planen Sie Aktualisierungen auf einem Dr.Web Server

1. Wählen Sie im Hauptmenü des **Verwaltungscenters** den Punkt **Administrierung**. Wählen Sie im geöffneten Fenster des Verwaltungsmenüs den Punkt **Dr.Web Server-Aufgabenplaner**. Die aktuelle Liste mit Aufgaben des **Servers** wird angezeigt.
2. Um eine Aufgabe der Liste hinzuzufügen, klicken Sie auf der Symbolleiste auf **Aufgabe erstellen**. Das Fenster für die Bearbeitung der Aufgaben wird geöffnet.
3. Geben Sie im Feld **Name** den Namen der Aufgabe ein, unter dem sie im Zeitplan angezeigt werden soll.
4. Wechseln Sie zur Registerkarte **Aktion** und wählen Sie in der Dropdown-Liste den Aufgabentyp **Repository aktualisieren**.

5. Aktivieren Sie in der angezeigten Liste die Kontrollkästchen neben den Komponenten, deren Aktualisierung geplant werden soll.
6. Wechseln Sie zur Registerkarte **Zeit**, wählen Sie in der Dropdown-Liste ein Intervall für die Häufigkeit der Aufgabenausführung und geben Sie anschließend den Zeitpunkt an, zu dem die Aufgabe ausgeführt werden soll.
7. Damit die vorgenommenen Änderungen wirksam werden, klicken Sie auf **Speichern**.

8.4. Repository von Dr.Web Server ohne Internetzugang aktualisieren

8.4.1. Repository von einem anderen Dr.Web Server kopieren

Wenn ein **Dr.Web Server** über keine Internetverbindung verfügt, können Sie sein Repository manuell aktualisieren, indem Sie das Repository eines bereits aktualisierten **Dr.Web Servers** kopieren.

Mit dieser Methode können Sie auf eine neuere Version nicht umsteigen.

So erhalten Sie Updates für die Antivirensoftware

1. Installieren Sie auf einem mit dem Internet verbundenen Rechner die Software des **Dr.Web Servers** wie in der **Installationsanleitung** unter Dr.Web Server installieren beschrieben.
2. Beenden Sie beide **Dr.Web Server**.
3. Um Updates für die Antivirensoftware zu erhalten, starten Sie den mit dem Internet verbundenen **Server**, indem Sie den Schalter `syncrepository` ausführen.

   Beispiel für **Windows**:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" syncrepository
```

4. Ersetzen Sie den ganzen Inhalt des Verzeichnisses vom Repository des **Hauptservers** (Arbeitsservers) durch den Inhalt des identischen Verzeichnisses vom Repository des **Servers**, der mit dem Internet verbunden ist. Das sind in der Regel:
   - `var\repository` unter **Windows**
   - `/var/drwcs/repository` unter **FreeBSD**
   - `/var/opt/drwcs/repository` unter **Linux** und **Solaris**

Wenn auf dem Rechner mit dem **Dr.Web Server** ein **Agent** mit der aktivierten Komponente **Dr.Web Selbstschutz** installiert ist, müssen Sie vor der Aktualisierung des Repository in den Einstellungen des **Agents** diese Komponente deaktivieren.

5. Wenn der **Hauptserver** unter einem UNIX-artigen Betriebssystem läuft, müssen die Rechte des Benutzers, der bei der Installation dieses **Servers** erstellt oder ausgewählt wurde, für das kopierte Repository festgelegt werden.
6. Führen Sie auf dem **Hauptserver** den folgenden Befehl aus:

```
drwcsd rerepository
```

   Ausgeführt werden kann der Befehl unter **Windows** über die *Befehlszeile*:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" rerepository
```

oder über das Menü `Start → Programme → Dr.Web Server → Serververwaltung → Repository neu starten`.

7. Starten Sie den **Hauptserver**.

Wenn Sie die Komponente **Dr.Web Selbstschutz** bei der Aktualisierung des Repository deaktiviert haben, sollten Sie diese Komponente wieder aktivieren.

8.4.2. Repository über das GUS herunterladen

Wenn der **Dr.Web Server** über keine Internetverbindung verfügt, können Sie sein Repository manuell aktualisieren, indem Sie das über das **GUS** heruntergeladene Repository importieren.

Um das Repository des **Dr.Web Servers** über das **GUS** herunterzuladen, verwenden Sie das Dienstprogramm **Dr.Web Repository Lader**.

Besonderheiten des Repository Loaders

- Um das Repository über das **GUS** herunterladen zu können, brauchen Sie einen gültigen Schlüssel für **Dr.Web Enterprise Security Suite** oder seinen MD5-Hash, der im **Verwaltungscenter** unter **Administrierung→ Lizenzmanager** angezeigt wird.
- **Dr.Web Repository Lader** steht Ihnen in den folgenden Oberflächen zur Verfügung:
  - In der grafischen Oberfläche (nur unter Windows)
  - In der Konsolenoberfläche
- Beim Herunterladen des Repository über das **GUS** kann ein Proxy-Server verwendet werden.

8.4.2.1. GUI-Dienstprogramm

Die GUI-Version des **Dr.Web Repository Laders** kann über das **Verwaltungscenter** im Bereich **Administrierung** → **Dienstprogramme** heruntergeladen werden. Dieses GUI-Dienstprogramm kann auf einem beliebigen Rechner unter Windows gestartet werden, der über eine Internetverbindung verfügt. Die entsprechende ausführbare Datei ist `drwreploader-gui-<Version>.exe`.

So laden Sie das Repository über die GUI-Version des Dr.Web Repository Laders herunter

1. Starten Sie die GUI-Version des **Dr.Web Repository Laders**.
2. Legen Sie im Hauptfenster des Dienstprogramms die folgenden Parameter fest:
   a) **Lizenzschlüssel oder MD5-Wert des Schlüssels**. Geben Sie hier die Datei eines **Dr.Web** Lizenzschlüssels an. Klicken Sie dafür auf **Durchsuchen** und wählen Sie eine gültige Lizenzschlüsseldatei. Alternativ können Sie den MD5-Hash des Lizenzschlüssels angeben, den Sie im **Verwaltungscenter** unter **Administrierung** → **Lizenzmanager** einsehen können.
   b) **Speicherort**. Geben Sie hier das Verzeichnis an, in welches das Repository heruntergeladen werden soll.
   c) Wählen Sie in der Liste **Modus** einen Modus für das Herunterladen von Updates aus:
      - **Repository laden**. Diese Option erzwingt das Herunterladen des Repository im Format des **Server**-Repository. Heruntergeladene Dateien können über das **Verwaltungscenter** als Updates des **Server**-Repository importiert werden.
      - **Aktualisierungsspiegel synchronisieren**. Diese Option erzwingt das Herunterladen des Repository als Update-Zone des **GUS**. Heruntergeladene Dateien können dann auf dem Update-Spiegel Ihres lokalen Netzwerks zur Verfügung gestellt werden. Sie können die **Server** so einstellen, dass sie Updates direkt von diesem Update-Spiegel, der jeweils die letzte Version des Repository enthält, beziehen.
   d) Aktivieren Sie das Kontrollkästchen **Repository archivieren**, um das heruntergeladene Repository in einem ZIP-Archiv zu komprimieren. Dadurch kann das heruntergeladene Repository am **Server** über das **Verwaltungscenter** unter **Administrierung** → Inhalt des Repository als eine ZIP-Datei importiert werden.
3. Wenn Sie die zusätzlichen Einstellungen für die Verbindung mit dem **GUS** und das Herunterladen von Updates ändern wollen, klicken Sie auf **Erweiterte Parameter**. Im angezeigten Fenster stehen Ihnen die folgenden Registerkarten zur Verfügung:
   a) Auf der Registerkarte **Produkte** können Sie die Liste der herunterzuladenden Produkte ändern. Im angezeigten Fenster werden alle zum Herunterladen über das **GUS** verfügbaren Repository-Produkte aufgelistet:
      - Um die Liste der im **GUS** aktuell verfügbaren Produkte zu aktualisieren, klicken Sie auf **Aktualisieren**.
      - Aktivieren Sie die Kontrollkästchen neben den Produkten, die Sie über das **GUS** herunterladen wollen. Um alle Produkte auszuwählen, aktivieren Sie das Kontrollkästchen in der Überschrift der Tabelle.
   b) Auf der Registerkarte **Dr.Web GUS** können Sie die Update-Server konfigurieren:
      - Alle **GUS**-Server werden in der Reihenfolge aufgelistet, in der sie vom Dienstprogramm Anforderungen beim Herunterladen des Repository erhalten. Um die Reihenfolge der **GUS**-Server zu ändern, verwenden Sie die Schaltflächen **Aufwärts** und **Abwärts**.
      - Um einen **GUS**-Server in die Liste der zum Herunterladen verwendeten Server aufzunehmen, geben Sie ins Feld oberhalb der Liste die Adresse des **GUS**-Servers ein und klicken Sie die Schaltfläche **Hinzufügen** an.
      - Um einen **GUS**-Server aus der Liste der verwendeten Server zu entfernen, wählen Sie die zu entfernenden Server aus und klicken Sie auf **Löschen**.
      - Geben Sie im Feld **Basis-URI** das Verzeichnis auf den Servern des **GUS** an, das Updates für **Dr.Web** Produkte beinhaltet.

- Wählen Sie in der Liste **Protokoll** das Protokoll aus, über das Updates aus Update-Servern heruntergeladen werden sollen. Updates werden dabei entsprechend den Einstellungen in der Liste der **GUS**-Server heruntergeladen.
- Wählen Sie in der Liste **Akzeptierte Zertifikate** den Typ von SSL-Zertifikaten, die automatisch angenommen werden sollen. Diese Einstellung ist nur für sichere Verbindungen verfügbar.
- **Anmeldename** und **Passwort**. Hier werden die Anmeldedaten des Benutzer angegeben, die bei der Authentifizierung (sofern erforderlich) am Update-Server verwendet werden sollen.
- Aktivieren Sie das Kontrollkästchen **CDN verwenden**, um Content Delivery Network beim Herunterladen des Repository zuzulassen.

c) Auf der Registerkarte **Proxy** können Sie eine Proxy-Verbindung mit dem **GUS** konfigurieren:
- **Adresse des Proxy-Servers** und **Port**. Hier werden die Netzwerkadresse und Portnummer des verwendeten Proxy-Servers angegeben.
- **Anmeldename** und **Passwort**. Hier werden die Einstellungen für die Autorisierung am Proxy-Server festgelegt, falls der verwendete Proxy-Server die Autorisierung erfordert.

d) Auf der Registerkarte **Planer** können Sie einen Update-Zeitplan einstellen. Dabei wird der Aufgabenplaner von Windows verwendet. Das Repository wird automatisch mit der festgelegten Häufigkeit heruntergeladen, ohne dass Sie das Tool manuell starten müssen.

e) Auf der Registerkarte **Protokoll** können Sie die Protokollierungseinstellungen festlegen.

Klicken Sie auf **OK**, um die vorgenommenen Änderungen zu übernehmen und zum Hauptfenster des **Dr.Web Repository Loaders** zurückzukehren.

4. Sobald Sie mit der Konfiguration fertig sind, klicken Sie im Hauptfenster des **Dr.Web Repository Laders** auf **Herunterladen**, um eine Verbindung mit dem **GUS** herzustellen und das Repository herunterzuladen.

8.4.2.2. Konsolendienstprogramm

Die Konsolenversion des Dienstprogramms **Dr.Web Repository Loader** befindet sich im Unterverzeichnis `bin` des Installationsverzeichnisses vom **Dr.Web Server**. Diese Version darf nur aus diesem Verzeichnis des **Servers** gestartet werden. Die entsprechende ausführbare Datei ist `drwreploader`.

Mögliche Anwendungsbeispiele

Empfohlene Vorgehensweise

1. Laden Sie vom **GUS** das Repository des **Servers** mithilfe des Dienstprogramms **Dr.Web Repository Lader** herunter. Verwenden Sie beim Herunterladen den Schalter `--archive`, um eine Archivdatei zu generieren.
2. Importieren Sie das heruntergeladene Repository über das **Verwaltungscenter** unter **Administrierung** → Inhalt des Repository in den **Server**.

Manueller Import

1. Laden Sie vom **GUS** das Repository des **Servers** mithilfe des Dienstprogramms **Dr.Web Repository Lader** herunter, ohne dass Sie den Schalter `--archive` verwenden. Verwenden Sie beim Herunterladen den Schalter `--path` *<Argument>*, um das Repository in das vorgegebene Verzeichnis zu importieren.
2. Um das Repository zu importieren, kopieren Sie dessen Inhalt, der sich im unter dem Parameter *<Argument>* angegebenen Verzeichnis befindet, in das Verzeichnis `/repository` des Installationsverzeichnisses vom **Server** und ersetzen Sie dadurch die dort vorhandenen Dateien.

3. Laden Sie erneut das Repository über das **Verwaltungscenter** unter **Administrierung** → Inhalt des Repository.

Zulässige Schalter

- `--help` – Hilfe zu Schaltern anzeigen.
- `--show-products` – Liste der im **GUS** verfügbaren Produkte anzeigen.
- `--path` <*Argument*> – das Repository über das **GUS** in das unter dem Parameter <*Argument*> angegebene Verzeichnis herunterladen.
- `--etc` <*Argument*> – Pfad zum Verzeichnis `etc` des **Servers** (wird zur Suche nach Stammzertifikaten und zum Update öffentlicher Schlüssel verwendet).
- `--archive` – das Repository in eine Archivdatei packen.
- `--key` <*Argument*> – Pfad zur Lizenzschlüsseldatei (ein Schlüssel oder sein MD5-Hash muss angegeben werden).
- `--key-md5` <*Argument*> – MD5-Hash eines Lizenzschlüssels (ein Schlüssel oder sein MD5-Hash muss angegeben werden).
- `--product` <*Argument*> – das zu aktualisierende Produkt. Standardmäßig wird das ganze Repository herunterladen.
- `--only-bases` – nur Virendatenbanken herunterladen.
- `--update-url` <*Argument*> – Verzeichnis auf den Servern des **GUS**, das Updates für **Dr.Web** Produkte beinhaltet (der Standardwert ist empfehlenswert).
- `--servers` <*Argument*> – Adressen der Server des **GUS** (der Standardwert ist empfehlenswert).
- `--prohibit-cdn` – das CDN beim Herunterladen der Updates verbieten (standardmäßig deaktiviert, da das CND zugelassen ist).
- `--prohibit-ssl` – nicht sichere HTTP-Verbindungen statt HTTPS-Verbindungen verwenden (standardmäßig deaktiviert, da HTTPS-Verbindungen verwendet werden).
- `--cert-mode` [<*Argument*>`]` – HTTPS-Zertifikate automatisch akzeptieren.

  <*Argument*> kann folgende Werte haben:

  - `any` – alle Zertifikate akzeptieren,
  - `valid` – nur vertrauenswürdige Zertifikate akzeptieren,
  - `drweb` – nur **Dr.Web** Zertifikate akzeptieren.

  Standardmäßig wird der Wert `drweb` verwendet.

- `--proxy-host` <*Argument*> – Proxy-Server im Format <*Server*>`[:`<*Port*>`]`.
- `--proxy-auth` <*Argument*> – Informationen für die Authentifizierung am Proxy-Server: der Anmeldename des Benutzers und das Passwort im Format <*Benutzer*>`[:`<*Passwort*>`]`.
- `--strict` – Herunterladevorgang bei einem Fehler abbrechen.
- `--log`<*Argument*> – Protokoll im Format eines **Server**-Protokolls zum Herunterladen des Repository erstellen und es im unter dem Parameter<*Argument*> angegebenen Verzeichnis ablegen.

Syntaxbeispiele

1. Eine importierbare Archivdatei mit allen Produkten erstellen:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --etc "C:\Program Files\DrWeb Server\etc"
```

2. Eine importierbare Archivdatei mit Virendatenbanken erstellen:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --only-bases --etc "C:\Program Files\DrWeb Server
\etc"
```

3. Eine importierbare Archivdatei mit nur dem **Server** erstellen:

```
drwreploader.exe --path=C:\Temp\repository.zip --archive --key "C:\Program Files
\DrWeb Server\etc\agent.key" --product=20-drwcs --etc "C:\Program Files\DrWeb
Server\etc"
```

8.5. Updates für Workstations einschränken

Über das **Verwaltungscenter** können Sie eine zeitgesteuerte Aktualisierung der auf den Workstations installierten Komponenten von **Dr.Web Enterprise Security Suite** konfigurieren.

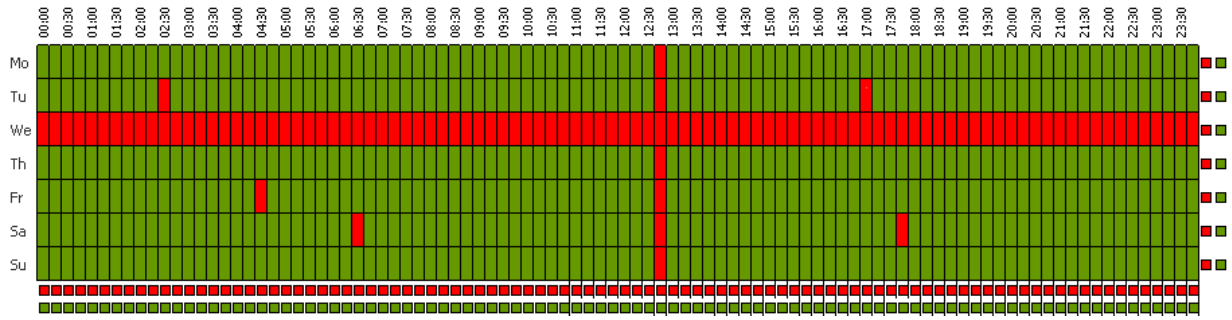
So konfigurieren Sie eine zeitgesteuerte Aktualisierung von Workstations

1. Wählen Sie im Hauptmenü den Punkt **Antivirus-Netzwerk**. Klicken Sie in der angezeigten hierarchischen Liste auf den Namen der gewünschten Workstation oder Gruppe. Wählen Sie im Verwaltungsmenü den Punkt **Update-Restriktionen**.
2. Wählen Sie in der Dropdown-Liste **Update-Restriktionen** einen Modus aus:
   - **Ohne Einschränkungen**. Diese Option gibt an, dass keine Einschränkungen für die Verteilung von Updates auf die Workstations vorgenommen werden sollen.
   - **Alle Updates verbieten**. Diese Option verbietet die Verteilung aller Updates in den in der Tabelle **Update-Zeitplan für Stationen** angegebenen Zeiträumen.
   - **Nur Datenbanken aktualisieren**. Diese Option verbietet die Verteilung von Updates für Programmmodule in den in der Tabelle **Update-Zeitplan für Stationen** angegebenen Zeiträumen. Virendatenbanken sind davon nicht betroffen und werden im normalen Modus aktualisiert.
3. Aktivieren Sie das Kontrollkästchen **Update-Traffic einschränken**, um das Volumen des Netzwerk-Datenverkehrs bei der Übertragung von Updates zwischen dem **Server** und den **Agents** einzuschränken. Geben Sie im Feld **Maximale Übertragungsgeschwindigkeit (KB/s)** die maximal zulässige Übertragungsrate für die Übertragung von Updates.

   Mehr dazu finden Sie unter Einschränkungen für die Übertragung von Updates.
4. Aktivieren Sie das Kontrollkästchen **Alle neusten Updates erhalten**, damit die Workstation trotz der im Bereich Detaillierte Konfiguration des Repository festgelegten Einschränkungen alle Updates ihrer Komponenten erhalten kann.

   Wenn das Kontrollkästchen deaktiviert ist, erhält die Workstation nur die Updates, die als aktuell zu verteilende Updates gelten.
5. In der Tabelle **Update-Zeitplan für Stationen** wird jeder Modus durch eine Farbe gekennzeichnet:
   - Grün – Aktualisierung ist zugelassen.
   - Rot – Aktualisierung ist verboten.

   Die Einstellung muss für jede Viertelstunde jedes Tages der Woche separat festgelegt werden.



Um den Aktualisierungsmodus zu ändern, klicken Sie auf die entsprechende Zelle der Tabelle.

- Um den Aktualisierungsmodus für eine ganze Zeile (für einen ganzen Tag) zu ändern, klicken Sie auf das entsprechende farbige Symbol rechts von der gewünschten Zeile der Tabelle.
- Um den Aktualisierungsmodus für eine ganze Spalte (für eine Viertelstunde jedes Tages) zu ändern, klicken Sie auf das entsprechende farbige Symbol unter der gewünschten Spalte der Tabelle.

6. Sobald Sie mit der Bearbeitung fertig sind, klicken Sie auf **Speichern**, um die vorgenommenen Änderungen zu übernehmen.

Auf der Symbolleiste sind die folgenden Optionen verfügbar:

Alle Parameter mit den ursprünglichen Werten wiederherstellen. Diese Option gibt an, dass die ursprünglichen (zuletzt gespeicherten) Werte aller Einstellungen des Bereichs wiederhergestellt werden sollen.

Defaultparameter wiederherstellen. Diese Option gibt an, dass die Standardwerte aller Einstellungen des Bereichs wiederhergestellt werden sollen.

Diese Einstellungen auf ein anderes Objekt verbreiten. Diese Option gibt an, dass die Einstellungen dieses Bereichs in die Einstellungen einer anderen Workstation, Gruppe oder einiger Gruppen und Workstations kopiert werden sollen.

Vererben von Einstellungen der primären Gruppe setzen. Diese Option gibt an, dass alle individuellen Einstellungen der Workstations durch die jeweiligen Einstellungen der primären Gruppe ersetzt werden sollen.

Einstellungen der primären Gruppe kopieren und diese als persönliche Einstellungen verwenden. Diese Option gibt an, dass die Einstellungen des Bereichs aus der primären Gruppe kopiert werden und auf den ausgewählten Workstations verwendet werden sollen. Die Vererbung findet dabei nicht statt, und die Einstellungen der Workstation gelten als individuell.

Einstellungen aus diesem Bereich in die Datei exportieren. Diese Option gibt an, dass alle Einstellungen des Bereichs in eine Datei gespeichert werden sollen.

Einstellungen aus der Datei in diesen Bereich importieren. Diese Option gibt an, dass alle Einstellungen des Bereichs durch die in einer speziellen Datei enthaltenen Einstellungen ersetzt werden sollen.

8.6. Mobile Dr.Web Agents aktualisieren

Wenn Ihr Rechner, Laptop oder mobiles Gerät längere Zeit keine Verbindung mit dem **Dr.Web Server** herstellen können, ist es empfehlenswert, den Mobilmodus des **Dr.Web Agents** zu aktivieren, um Updates über das **Dr.Web GUS** rechtzeitig erhalten zu können.

Im Mobilmodus versucht der **Agent** bis zu dreimal, eine Verbindung mit dem **Server** herzustellen. Wenn diese Versuche nicht erfolgreich sind, wird eine Aktualisierung über HTTP durchgeführt. Suchvorgänge nach dem **Server** erfolgen permanent im Abstand von ca. 1 Minute.

Der Mobilmodus kann über die Einstellungen des **Agents** aktiviert werden, vorausgesetzt, dass der Mobilmodus für das **Dr.Web GUS** in den Berechtigungen der Workstation erlaubt ist (weitere Informationen finden Sie unter Benutzerrechte konfigurieren).

Wenn sich der **Agent** im Mobilmodus befindet, wird die Kommunikation zwischen dem **Agent** und **Dr.Web Server** abgebrochen. Alle Änderungen, die auf dem **Server** für die involvierte Workstation festgelegt werden, werden erst dann wirksam, wenn der Mobilmodus des **Agents** deaktiviert wird und der **Agent** mit dem **Server** erneut verbunden ist.

Im Mobilmodus werden nur Virendatenbanken aktualisiert.

Die Beschreibung der Einstellungen vom Mobilmodus des **Agents** können Sie im **Benutzerhandbuch** finden.

Kapitel 9: Zusätzliche Komponenten konfigurieren

9.1. Proxy-Server

Ein Antivirus-Netzwerk kann ein bzw. mehrere **Proxy-Server** umfassen.

Ein **Proxy-Server** dient hauptsächlich dazu, eine sichere Kommunikation zwischen dem **Dr.Web Server** und den **Dr.Web Agents** zu gewährleisten, wenn keine direkte Verbindung hergestellt werden kann. Das kann der Fall sein, wenn sich der **Dr.Web Server** und die **Dr.Web Agents** in verschiedenen Netzwerken befinden, sodass kein Paketrouting möglich ist.

Um eine sichere Kommunikation zwischen dem **Server** und den Clients über einen **Proxy-Server** zu ermöglichen, sollten Sie die Verschlüsselung des Datenverkehrs deaktivieren. Wählen Sie dafür den Wert **Nein** für den Parameter **Verschlüsselung** im Bereich Dr.Web Server-Konfiguration > Allgemein aus.

Grundlegende Funktionen

Proxy-Server erfüllt die folgenden Funktionen:

1. hört das Netzwerk ab und empfängt die von über das festgelegte Protokoll und den Port aufgebauten Verbindungen;
2. übersetzt Protokolle (unterstützt werden TCP/IP-Protokolle);
3. überträgt Daten zwischen dem **Dr.Web Server** und den **Dr.Web Agents** entsprechend den Einstellungen des **Proxy-Servers;**
4. zwischenspeichert Updates des **Agents** und des Antivirenpakets, die vom **Server** übertragen werden. Der Zugriff auf die vom **Proxy-Server** zwischengespeicherten Updates bringt die folgenden Vorteile:
   - Reduzierung des Netzwerkdatenverkehrs,
   - wesentlich schnellere Aktualisierung der **Agents**.

Mehrere **Proxy-Server** können zu einem hierarchischen Verbund zusammengeschaltet werden.

Einen allgemeinen Plan des Antivirus-Netzwerks bei der Verwendung eines **Proxy-Servers** finden Sie in der Abb. 9-1.

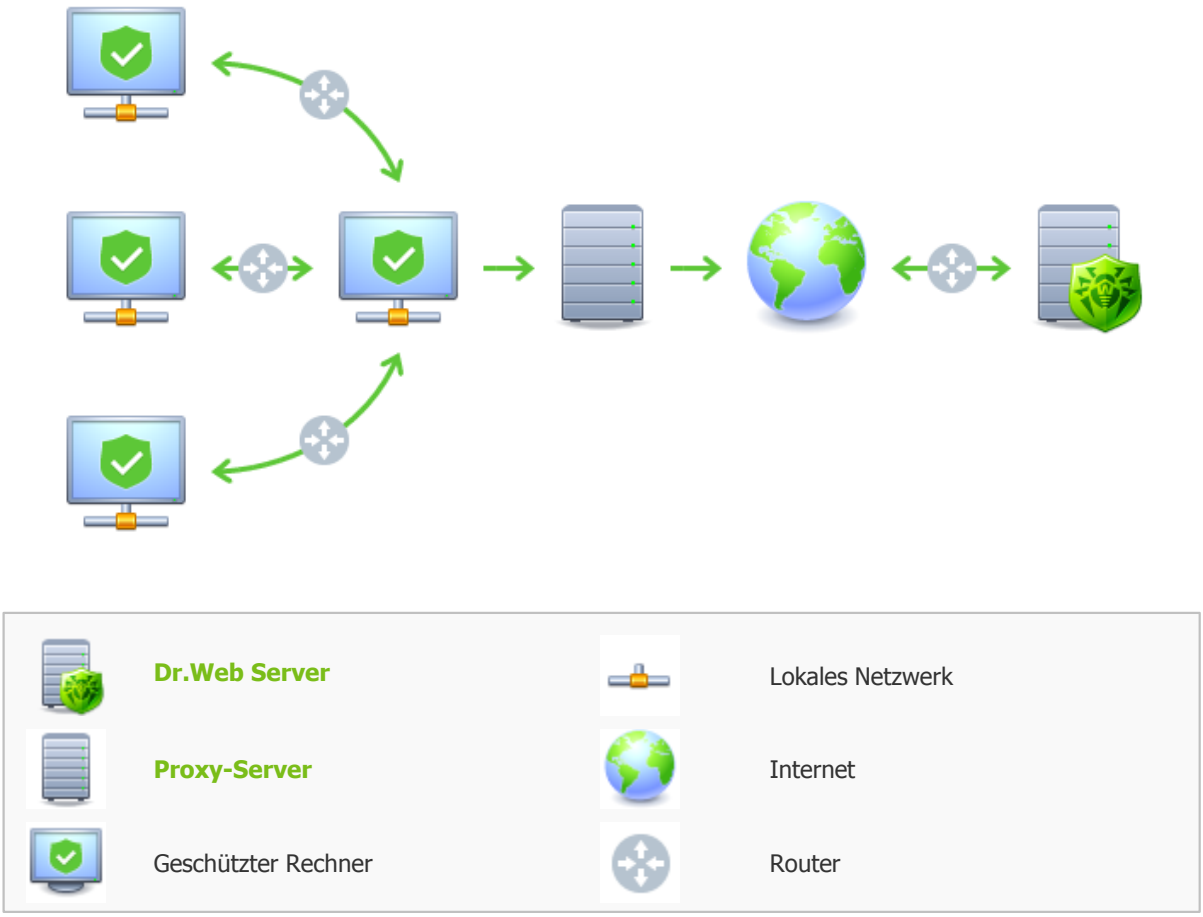


Abbildung 9-1: Plan des Antivirus-Netzwerks bei der Verwendung eines Proxy-Servers

Funktionsweise

Bei der Verwendung eines Proxy-Servers werden die folgenden Aktionen ausgeführt:

1. Wenn die Adresse des **Servers** im **Agent** nicht angegeben ist, sendet der **Agent** über das im Netzwerk verwendete Protokoll eine Multicast-Anfrage.
2. Wenn der **Proxy-Server** für die Übersetzung von Protokollen (Parameter `discovery="yes"`) eingestellt ist, erhält der **Agent** eine Nachricht darüber, dass ein **Proxy-Server** verfügbar ist.
3. Der **Agent** verwendet die erhaltenen Parameter des **Proxy-Servers** als Parameter des **Dr.Web Servers**. Weitere Kommunikation erfolgt für den **Agent** transparent.
4. Entsprechend den Parametern der Konfigurationsdatei lauscht der **Proxy-Server** an den festgelegten Ports auf die eingehenden Verbindungen, die über die angegebenen Protokolle erfolgen.
5. Für jede eingehende Verbindung vom **Agent** stellt der **Proxy-Server** eine Verbindung mit dem **Dr.Web Server** her.

Weiterleitungsalgorithmus bei der Verwendung einer Liste von Dr.Web Servern:

1. Der **Proxy-Server** lädt in den Arbeitsspeicher die Liste der **Dr.Web Server**, die in der Konfigurationsdatei `drwcsd-proxy.xml` angegeben sind (s. dazu im Dokument **Anhänge** den Anhang G4).
2. Der **Dr.Web Agent** verbindet sich mit dem **Proxy-Server**.
3. Der **Proxy-Server** leitet den **Dr.Web Agent** an den als ersten in der Liste im Arbeitsspeicher stehenden **Dr.Web Server** weiter.

4. Der **Proxy-Server** rotiert die im Arbeitsspeicher befindliche Liste und verschiebt den **Dr.Web Server** an das Ende der Liste.

Der **Proxy-Server** kann die geänderte Reihenfolge der **Server** in seiner Konfigurationsdatei nicht speichern. Bei einem Neustart des **Proxy-Servers** wird die Liste der **Dr.Web Server** in ihrer ursprünglichen Form, wie sie in der Konfigurationsdatei gespeichert ist, geladen.

5. Wenn ein anderer **Agent** eine Verbindung mit dem **Proxy-Server** herstellt, wiederholt sich der Vorgang vom Schritt 2 an.
6. Wenn der **Dr.Web Server** die Verbindung mit dem Antivirus-Netzwerk trennt (z. B. beim Ausschalten oder einer Dienstverweigerung), stellt der **Agent** erneut eine Verbindung mit dem **Proxy-Server** her. Der Vorgang wiederholt sich dabei vom Schritt 2 an.

Netzwerk-Scanner, der auf einem Rechner in einem externen Netzwerk (relativ zu den **Agents** des Netzwerks) gestartet wurde, kann die installierten **Agents** nicht finden.

Wenn das Kontrollkästchen **NetBIOS-Namen ersetzen** aktiviert ist und ein **Proxy-Server** im Antivirus-Netzwerk verwendet wird, wird der Name des Rechners, auf dem der **Proxy-Server** installiert ist, für alle Workstations, die mit dem **Server** über den **Proxy-Server** verbunden sind, im **Verwaltungscenter** verwendet.

Verschlüsselung und Komprimierung des Datenverkehrs

Proxy-Server kann sowohl komprimiert als auch nicht komprimiert übertragene Daten verarbeiten.

Der **Proxy-Server** kann keine verschlüsselt übertragenen Daten verarbeiten. Er analysiert übertragene Informationen und wechselt in den transparenten Modus, wenn der Datenverkehr zwischen dem **Dr.Web Server** und dem **Agent** verschlüsselt wird, d. h. der **Proxy-Server** überträgt den ganzen Datenverkehr zwischen dem **Server** und **Agent**, ohne die übertragenen Daten zu verarbeiten.

Wenn der Datenverkehr zwischen dem **Agent** und **Server** verschlüsselt wird, werden im **Proxy-Server** keine Updates zwischengespeichert.

Zwischenspeichern

Proxy-Server kann übertragene Daten zwischenspeichern.

Produkte werden in Revisionen zwischengespeichert. Jede Revision wird in einem einzelnen Verzeichnis abgelegt. Das Verzeichnis jeder weiteren Revision enthält *feste Links* (*hard links*) auf die vorhandenen Dateien der alten Revisionen und die ursprünglichen Dateien der modifizierten Dateien. Also, nur eine Kopie der Dateien jeder Version wird auf der Festplatte gespeichert. In allen Verzeichnissen weiterer Revisionen befinden sich nur Links auf die modifizierten Dateien.

Falls das Zwischenspeichern aktiviert ist, ermöglichen die in der Konfigurationsdatei festzulegenden Einstellungen die folgenden Aktionen:

- Regelmäßiges Löschen nicht aktueller Revisionen. Standardmäßig werden sie stündlich gelöscht.
- Speichern nur der aktuellsten Revisionen. Alle älteren Revisionen gelten als nicht aktuell und werden gelöscht. Standardmäßig werden nur drei letzte Revisionen gespeichert.
- Periodisches Entladen nicht verwendeter *Memory-Mapped*-Dateien. Standardmäßig werden sie alle 10 Minuten entladen.

Einstellungen

Der **Proxy-Server** hat keine grafische Oberfläche. Alle Einstellungen werden mithilfe einer Konfigurationsdatei vorgenommen. Das Format der Konfigurationsdatei des **Proxy-Servers** wird im Dokument **Anhänge** unter Anhang G4 detailliert beschrieben.

Um die Konfigurationsdatei des **Proxy-Servers** bearbeiten zu können, müssen Sie als Administrator am Rechner angemeldet sein.

Damit ein **Proxy-Server** unter einem der Linux-basierten Betriebssysteme funktionsfähig ist, müssen Sie nach einem Neustart des Rechners die Netzwerkkonfiguration einstellen, ohne den Netzwerk-Manager zu verwenden.

Starten und Beenden

Unter Windows wird der **Proxy-Server** mit Windows-Bordmittel gestartet und angehalten. Doppelklicken Sie dafür unter **Systemsteuerung** → **Verwaltung** → **Dienste** → auf **drwcsd-proxy** und wählen Sie im geöffneten Fenster die gewünschte Aktion aus.

Unter Betriebssystemen der UNIX-Familie wird der **Proxy-Server** über die `start`- und `stop`-Skripts, die bei der Installation des **Proxy-Servers** erstellt wurden, gestartet und angehalten (mehr dazu finden Sie in der **Installationsanleitung** unter Proxy-Server installieren).

Alternativ können Sie zum Start eines **Proxy-Servers** unter Windows bzw. einem der UNIX-basierten Betriebssysteme die ausführbare Datei `drwcsd-proxy` mit den entsprechenden Parametern starten (mehr dazu finden Sie unter Anhang H8. Proxy-Server).

9.2. NAP Validator

Allgemeine Informationen

Microsoft® Network Access Protection (Netzwerkzugriffsschutz) ist eine Gruppe von Betriebssystemkomponenten in einigen Windows-Betriebssystemen, mit denen Sie Ihr Netzwerk besser schützen können. Der bessere Schutz des Netzwerks wird dadurch ermöglicht, dass mit dieser Plattform überprüft werden kann, ob Workstations den vom Administrator definierten Anforderungen für die Systemintegrität entsprechen.

Bei der Verwendung der NAP-Technologie können Sie benutzerdefinierte Integritätsanforderungsrichtlinien für die Überprüfung der Clientintegrität erstellen. Ergebnisse der Auswertung werden in den folgenden Fällen analysiert:

- Bevor Zugriff bzw. Kommunikation zugelassen wird.
- Zur automatischen Wartung der als konform eingeschätzten Rechner, damit ihre Kompatibilität permanent sichergestellt wird.
- Zur Erzwingung der Kompatibilität mit den Integritätsanforderungen für nicht kompatible Rechner.

Weitere Informationen zur NAP-Technologie finden Sie auf dieser Webseite von Microsoft.

NAP-Technologie in Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite verwendet die NAP-Technologie, um die Integrität der Antivirensoftware auf den zu schützenden Workstations zu überprüfen. Zu diesem Zweck wird die Komponente **Dr.Web NAP Validator** eingesetzt.

Bei der Integritätsüberprüfung werden die folgenden Komponenten verwendet:

- Ein installierter und konfigurierter NAP-Integritätsrichtlinienserver.
- **Dr.Web NAP Validator**. Das ist eine Komponente, mit der die Integrität der Antivirensoftware des zu schützenden Systems (System Health Validator – SHV) anhand benutzerdefinierter **Dr.Web**-Integritätsrichtlinien überprüft wird. Diese Komponente wird auf dem Rechner installiert, der die Rolle eines NAP-Integritätsprüfungsservers ausübt.
- Systemintegritäts-Agent (System Health Agent – SHA). Diese Komponente wird auf der Workstation zusammen mit der Software des **Dr.Web Agents** installiert.
- **Dr.Web Server** dient als Wartungsserver, der die Integrität der Antivirensoftware auf den Workstations sicherstellt.

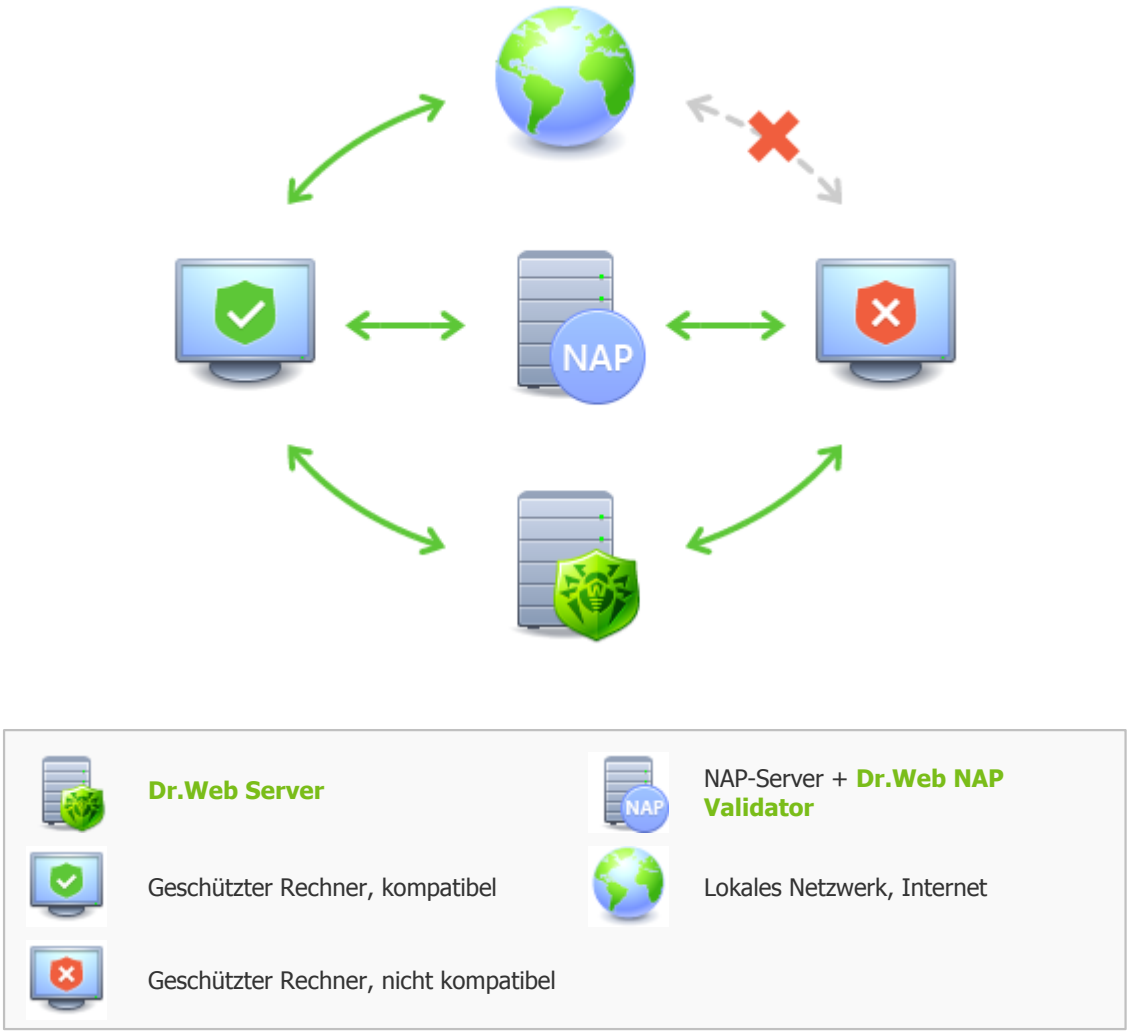


Abbildung 9-2: Plan des Antivirus-Netzwerks bei der NAP-Erzwingung

Die Integrität wird wie folgt überprüft:

1. Damit die Integrität und die Richtlinienkompatibilität überprüft werden können, aktivieren Sie in den Einstellungen des **Agents** die entsprechende Option (mehr dazu finden Sie unter Dr.Web Agent konfigurieren).
2. Der SHA auf der Workstation stellt eine Verbindung mit der Komponente **Dr.Web NAP Validator** her, die auf dem NAP-Server installiert ist.
3. **Dr.Web NAP Validator** überprüft die Integritätsrichtlinien (s. unten). Der **NAP Validator** überwacht und meldet den Integritätsstatus der Antivirensoftware, sodass der Netzwerkrichtlinienserver ermitteln kann, ob diese aktuell und richtig konfiguriert ist. Aufgrund der Integritätsinformationen werden alle NAP-fähigen Workstations in zwei Kategorien unterteilt:
   - Workstations, die den Richtlinienbedingungen entsprechen, werden als kompatibel mit den Netzwerkintegritätsanforderungen eingeschätzt und erhalten uneingeschränkten Zugriff auf das Netzwerk.
   - Workstations, die mindestens einer der Richtlinienbedingungen nicht entsprechen, werden als nicht kompatibel mit den Netzwerkintegritätsanforderungen eingeschätzt. Diese Workstations können nur auf den **Dr.Web Server** zugreifen und werden im eingeschränkten Netzwerk platziert. Nicht kompatible Workstations werden mithilfe des **Servers** gewartet, damit sie den Integritätsrichtlinien entsprechen. Anschließend wird der Integritätsstatus gewarteter Workstations erneut überprüft.

Integritätsanforderungen:

1. **Dr.Web Agent** muss gestartet und funktionsfähig sein.
2. Virendatenbanken müssen aktuell sein, d. h. sie müssen mit den Datenbanken auf dem Server übereinstimmen.

NAP Validator konfigurieren

Nach der Installation vom **Dr.Web NAP Validator** (s. dazu in der **Installationsanleitung** den Abschnitt NAP Validator installieren) auf dem Rechner mit dem installierten NAP-Server müssen Sie die folgenden Aktionen durchführen:

1. Öffnen Sie die Konfigurationskomponente des NAP-Servers (führen Sie dazu den Befehl `nps.msc` aus).
2. Wählen Sie im Bereich **Richtlinien** den Unterpunkt **Integritätsrichtlinien** aus.
3. Öffnen Sie im geöffneten Fenster die Eigenschaften der Elemente:
   - **NAP DHCP Compliant**. Aktivieren Sie im Einstellungsfenster das Kontrollkästchen **Dr.Web System Health Validator**, um die Richtlinien vom **Dr.Web NAP Validator** zu verwenden. Wählen Sie in der Dropdown-Liste den Punkt **Client passed all SHV checks**, damit die Workstation als kompatibel mit den Netzwerkintegritätsanforderungen eingestuft werden kann, wenn sie allen Richtlinienbedingungen entspricht.
   - **NAP DHCP Noncompliant**. Aktivieren Sie im Einstellungsfenster das Kontrollkästchen **Dr.Web System Health Validator**, um die Richtlinien vom **Dr.Web NAP Validator** zu verwenden. Wählen Sie in der Dropdown-Liste den Punkt **Client fail one or more SHV checks**, damit die Workstation als nicht kompatibel mit den Netzwerkintegritätsanforderungen eingestuft werden kann, wenn sie mindestens einer der Richtlinienbedingungen nicht entspricht.

Schlagwortregister

A

Administratoren
- Rechte 68

Agent
- Benutzeroberfläche 29
- Einstellungen 108
- Funktionen 29
- Mobilmodus 202
- Update 202

Anfänger 89, 108
Antivirenscanner 116
Antivirus-Netzwerk 183
- erkannte Bedrohungen 190
- Komponenten 55
- Struktur 55, 184
- Updates 190
- Verbindungen konfigurieren 186

Antivirus-Server
- Benutzeroberfläche 24, 26
- Einstellungen 136
- Inhalt des Verzeichnisses 24, 26
- Protokoll 23
- Start 26, 28
- Verbindungen konfigurieren 186
- Verbindungstypen 184
- Zeitplan 152

Aufgabenplaner
- Server 152

Automatische Autorisierung 43
Autorisierung, Verwaltungscenter 43

B

Basisdistribution des Dr.Web Servers
- Umfang 20

Benachrichtigungen
- Einstellung 164

Benutzeroberfläche
- Antivirus-Server 24, 26

Berechtigungen
- Administratoren 68

D

Datenbank
- Einstellungen 145

Datenverkehr
- Komprimierung 139
- Umfang 56
- Verschlüsselung 139

Datenverkehr-Kompression 139
Demoschlüssel 22
Distribution 20
Distributionsumfang 20
Dr.Web Server
- Aufgaben 23
- Benutzeroberfläche 24, 26
- Einstellungen 136
- Inhalt des Verzeichnisses 24, 26
- Protokoll 23
- Start 26, 28
- Verbindungen konfigurieren 186
- Verbindungstypen 184
- Zeitplan 152

E

Einstellungen
- Agent 108
- Antivirus-Server 136
- Einstellungen, Kopieren 87

Erstellen
- Gruppen 79

F

Funktionen
- Agent 29
- Dr.Web Server 23

G

Gruppen 76
- Einstellungen 84
- Einstellungen, Kopieren 87
- Einstellungen, Vererbung 86
- primäre 86
- Workstations hinzufügen 81
- Workstations löschen 81

GUS
- s. auch manuelle Aktualisierung 195

K

Komponenten
- Antivirus-Netzwerk 55
- Synchronisierung 195

Schlagwortregister

Konfiguration
- Agent 108
- Antivirus-Server 136

Konten 68

L

Lizenzierung 21

Löschen
- Gruppen 79
- Löschen aus der Gruppe 81
- Workstation 90

M

manuelle Aktualisierung 195

Mobilmodus des Agents 202

N

Nachrichten
- Logo-Format 134
- Versand an Benutzer 132

NAP Validator 207
- Einstellung 209

nicht bestätigte Workstations 89

P

primäre Gruppen 86

Protokoll des Servers 23

Proxy-Server
- Funktionalität 204
- Starten, Beenden 207

Q

Quarantäne 129

R

Rechte
- Administratoren 68

Registrierung
- des Dr.Web Produktes 21
- Workstations auf dem Server 89

Repository
- allgemeine Parameter 171
- vereinfachter Editor 172

Repository Loader 197

S

Scannen
- automatisch 100
- manuell 116

Scanner
- Antivirus 116
- Netzwerke 44

Schlüssel 21
- Demo 22
- Lizenz erhalten 21
- siehe auch Registrierung 21

Serververzeichnis, Inhalt 24, 26

Sprache
- Verwaltungscenter 41, 71

Start
- Dr.Web Server 26, 28

Statistik
- Workstation 124

Symbole
- hierarchische Liste 36
- Netzwerk-Scanner 46

Synchronisierung, Komponenten 195

Systemanforderungen 16

U

Update
- Agent 202
- Antivirus-Netzwerk 190
- Dr.Web Enterprise Security Suite 193
- Einschränkung 201
- manuell 195
- Mobilmodus 202
- nach Zeitplan 195
- zwangsläufig 195

Updates einschränken 201

V

Verbindungen, zwischen den Servern
- Einstellung 186
- Typen 184

Verschlüsselung
- Datenverkehr 139

Verwaltungscenter
- Beschreibung 30
- Eigenschaftenfenster 40

Schlagwortregister

Verwaltungscenter
- Hauptmenü 31
- hierarchische Liste 35
- Suchleiste 32
- Symbolleiste 37

Virenprüfung 116
vordefinierte Gruppen 76

W

Workstation
- Anfänger 89
- Aufnahme in Gruppe 81
- Aus Gruppe entfernen 81
- Einstellungen, Kopieren 87
- Einstellungen, Vererbung 86
- Löschen 90
- nicht bestätigt 89
- Scannen 100, 116
- Statistik 124
- Verbindung 89
- Verwaltung 89
- Wiederherstellen 90

Workstation wiederherstellen 90
Workstations verbinden 89

Z

Zeitplan
- des Servers 152
- Updates 195

zusätzliche Distribution des Dr.Web Servers
- Umfang 20

zwangsläufige Aktualisierung 195

© Doctor Web, 2015